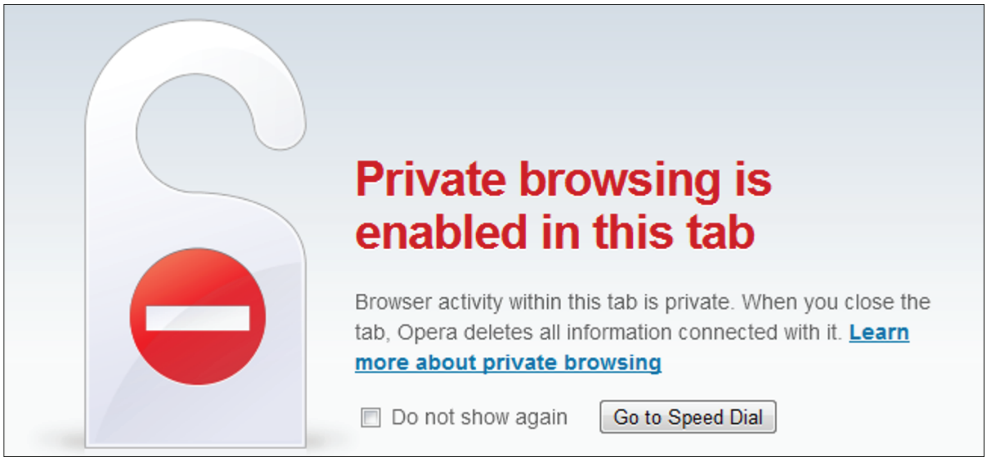
EXHIBIT 106

How-To Geek

How Private Browsing Works, and Why It Doesn't Offer Complete Privacy

CHRIS HOFFMAN @chrisbhoffman
UPDATED JUL 5, 2017, 12:26 PM EDT | 3 MIN READ



Private browsing is enabled in this tab

Browser activity within this tab is private. When you close the tab, Opera deletes all information connected with it. Learn more about private browsing

☐ Do not show again   Go to Speed Dial

Private Browsing, InPrivate Browsing, Incognito Mode – it has a lot of names, but it's the same basic feature in every browser. Private browsing offers some improved privacy, but it's not a silver bullet that makes you completely anonymous online.

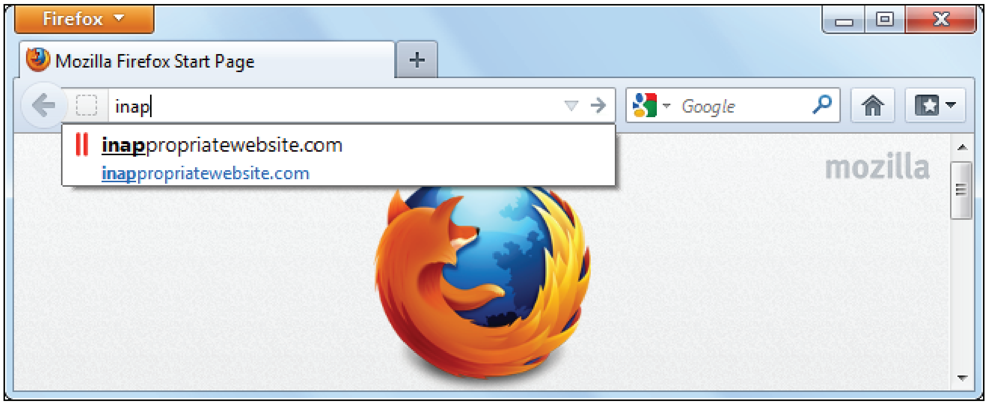
Private Browsing mode changes the way your browser behaves, whether you're using Mozilla Firefox, Google Chrome, Internet Explorer, Apple Safari, Opera or any other browser – but it doesn't change the way anything else behaves.

What Browsers Normally Do

When you browse normally, your web browser stores data about your browsing history. When you visit a website, your browser logs that visit in your browser history, saves cookies from the website, and stores form data it can autocomplete later. It also saves other information, such as a history of files you've downloaded, passwords you've chosen to save, searches you've entered in your browser's address bar, and bits of web pages to speed page load times in the future (also known as the cache).

Someone with access to your computer and browser could stumble across this information later – perhaps by typing something into your address bar and your web browser suggesting a website you've visited. Of course, they could also open your browsing history and view the lists of pages you've visited.

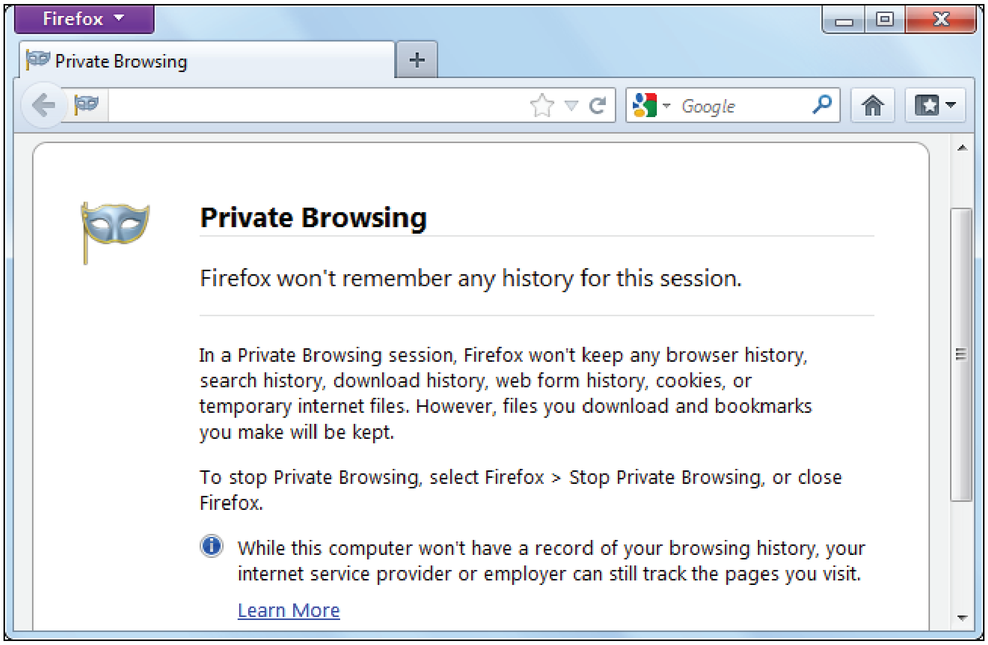
You may be able to disable some of this data collection in your browser, but this is the way the default settings work.



What Private Browsing Does

When you enable Private Browsing mode – also known as Incognito Mode in Google Chrome and InPrivate Browsing in Internet Explorer – your web browser doesn't store this information at all. When you visit a website in private-browsing mode, your browser won't store any history, cookies, form data – or anything else. Some data, like cookies, may be kept for the duration of the private browsing session and immediately discarded when you close your browser.

When private-browsing mode was first introduced, websites could get around this limitation by storing cookies using the Adobe Flash browser plug-in, but Flash now supports private browsing and won't store data when private-browsing mode is enabled.



Private Browsing

Firefox won't remember any history for this session.

In a Private Browsing session, Firefox won't keep any browser history, search history, download history, web form history, cookies, or temporary internet files. However, files you download and bookmarks you make will be kept.

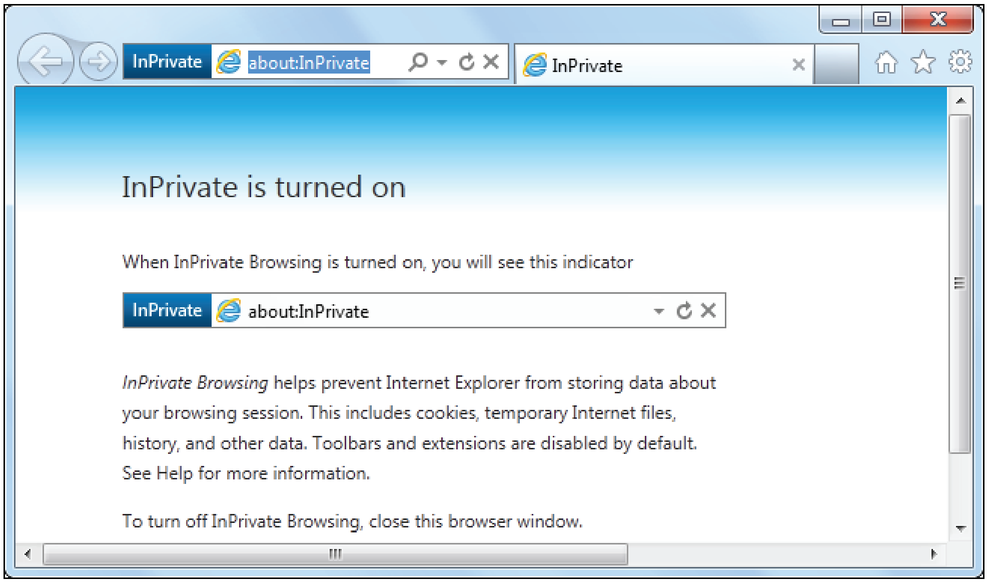
To stop Private Browsing, select Firefox > Stop Private Browsing, or close Firefox.

While this computer won't have a record of your browsing history, your internet service provider or employer can still track the pages you visit.

Learn More

Private browsing also functions as a completely isolated browser session – for example, if you're logged into Facebook in your normal browsing session and open a private-browsing window, you won't be logged into Facebook in that private-browsing window. You can view sites with Facebook integration in the private-browsing window without Facebook tying the visit to your logged-in profile. This also allows you to use the private-browsing session to log into multiple accounts at once – for example, you could be logged into a Google account in your normal browsing session and log into another Google account in the private-browsing window.

Private browsing protects you from people with access to your computer snooping at your browsing history – your browser won't leave any tracks on your computer. It also prevents websites from using cookies stored on your computer to track your visits. However, your browsing is not completely private and anonymous when using private-browsing mode.



InPrivate is turned on

When InPrivate Browsing is turned on, you will see this indicator

InPrivate Browsing helps prevent Internet Explorer from storing data about your browsing session. This includes cookies, temporary Internet files, history, and other data. Toolbars and extensions are disabled by default. See Help for more information.

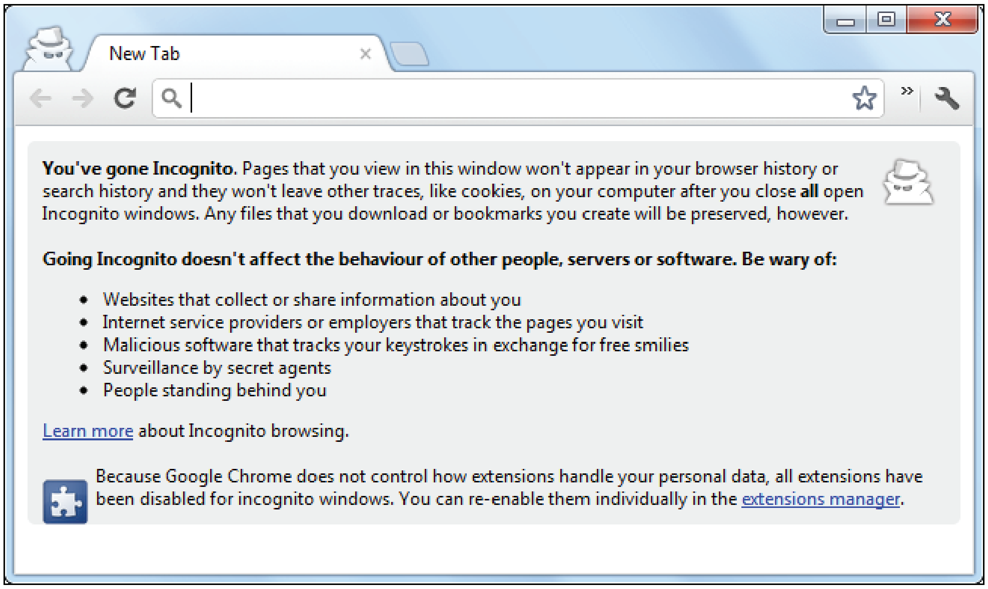
To turn off InPrivate Browsing, close this browser window.

Threats On Your Computer

Private Browsing prevents your web browser from storing data about you, but it doesn't stop other applications on your computer from monitoring your browsing. If you have a key logger or spyware application running on your computer, that application could monitor your browsing activity. Some computers may also have special monitoring software that tracks web browsing installed on them –

private browsing won't protect you against parental-control-type applications that take screenshots of your web browsing or monitor the websites you access.

Private browsing prevents people from snooping on your web browsing after it's occurred, but they can still snoop while it's occurring – assuming they have access to your computer. If your computer is secure, you shouldn't have to worry about this.



You've gone Incognito. Pages that you view in this window won't appear in your browser history or search history and they won't leave other traces, like cookies, on your computer after you close **all** open Incognito windows. Any files that you download or bookmarks you create will be preserved, however.

Going Incognito doesn't affect the behaviour of other people, servers or software. Be wary of:

- Websites that collect or share information about you
- Internet service providers or employers that track the pages you visit
- Malicious software that tracks your keystrokes in exchange for free smilies
- Surveillance by secret agents
- People standing behind you

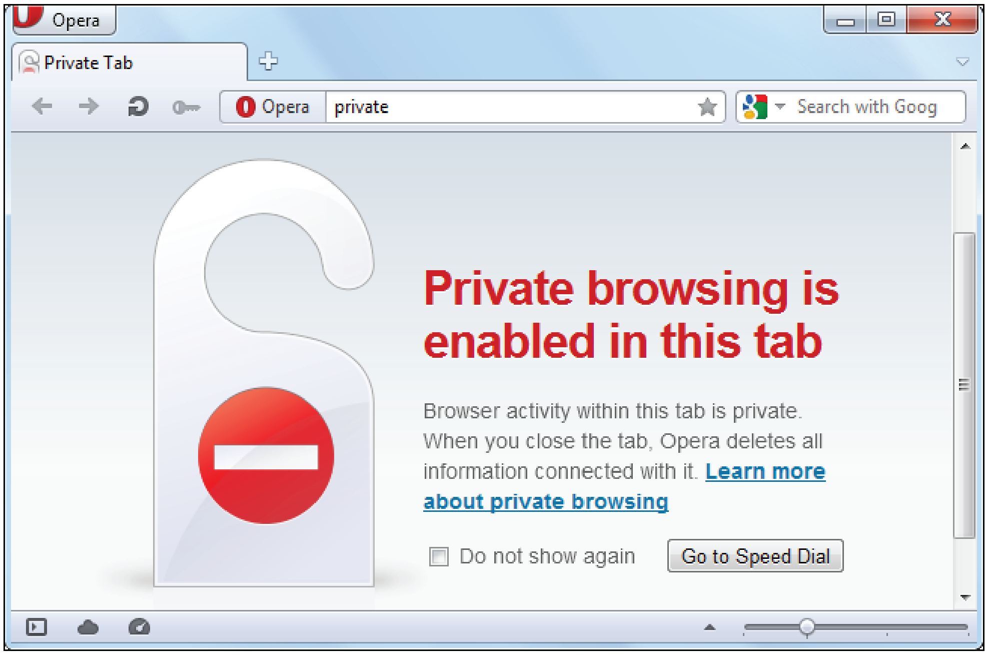
Learn more about Incognito browsing.

Because Google Chrome does not control how extensions handle your personal data, all extensions have been disabled for incognito windows. You can re-enable them individually in the extensions manager.

Network Monitoring

Private browsing only affects your computer. Your web browser can decide not to store browsing activity history on your computer, but it can't tell other computers, servers, and routers to forget your browsing history. For example, when you visit a website, the traffic leaves your computer and travels through several other systems to reach the website's server. If you're on a corporate or educational network, this traffic goes through a router on the network – your employer or school can log the website access here. Even if you're on your own network at home, the request goes through your Internet service provider – your Internet Service provider can log the traffic at this point. The request then reaches the website's server itself, where the server can log your access.

Private browsing doesn't stop any of this logging. It doesn't leave any history lying around on your computer for people to see, but your history can always be – and usually is — logged elsewhere.



Private browsing is enabled in this tab

Browser activity within this tab is private. When you close the tab, Opera deletes all information connected with it. Learn more about private browsing

If you really want to browse the web anonymously, try downloading and using Tor.

CHRIS HOFFMAN

Chris Hoffman is Editor-in-Chief of How-To Geek. He's written about technology for over a decade and was a PCWorld columnist for two years. Chris has written for The New York Times, been interviewed as a technology expert on TV stations like Miami's NBC 6, and had his work covered by news outlets like the BBC. Since 2011, Chris has written over 2,000 articles that have been read nearly one billion times---and that's just here at How-To Geek. **READ FULL BIO »**

The above article may contain affiliate links, which help support How-To Geek.

How-To Geek is where you turn when you want experts to explain technology. Since we launched in 2006, our articles have been read more than 1 billion times. Want to know more?

EXHIBIT 107

Private Browsing Won't Protect You From Everything

Private browsing gets rid of your browsing history, saved passwords, and field content. But if you think it keeps you safe from malware, ads, and ISP monitoring, think again.

By Ben Dickson
September 16, 2019

In the past several years, most internet browsers have added a private browsing mode aimed at protecting user privacy. Chrome calls it Incognito Mode; it's Private Browsing in Opera, Safari, and Firefox.

Characterized by dark-color themes and icons of masked figures, these modes can give a user the impression they're browsing anonymously. Researchers at the University of Chicago and Leibniz University of Hannover found that many users think private browsing will protect them against malware, advertising, tracking scripts, and monitoring by internet service providers (ISPs).

Nothing could be further from the truth. Here's what private browsing does and doesn't do.

What Does Private Browsing Hide?

Cookies, those bits of data stored in the browser that enable websites to keep track of user information, let you stay logged into your online accounts when you open your browser. For some websites, cookies also keep track of settings you configure, such as language, layout, and themes.

Private browsing is designed to avoid keeping traces of your browsing session on your computer. So when you open a private window, cookies from your main browsing window aren't carried over. And when you close the private browsing window, all cookies you generated during your session will be destroyed.

In theory, without cookies, websites can't identify you. So opening a new private browsing window should make you appear to the internet as a new user.

In practice, however, websites can still discover your identity by correlating other information, such as your IP address, device types, and browsing habits (time of day, pages visited, and so on). Private browsing hides *none* of that data. Big tech companies such as Facebook and Google have plenty of information about users, and by connecting the dots, they can identify you, even if you haven't logged into your account.

After you close a private browsing window, your browsing history, saved passwords, and the content you type in text fields (usernames, phone numbers, and so on) for that window is wiped. This means that the next person who sits behind your computer and fires up the browser will not be able to find out which websites you visited during your private browsing session.

But if you bookmark a page when you're in private browsing mode, it will be added to the bookmarks of your normal browsing page and will be visible to everyone. Also note that files you download to your computer while privately browsing will not be deleted when you close the window.

Can Your ISP See What You Search in Incognito?

This is one area in which private browsing won't protect you at all. Your ISP, corporate network administrator, and government agencies will be able to track your browsing habits regardless of the browsing mode you're using.

As your gateway to the internet, ISPs and network administrators control your traffic at the network level and can keep track of the websites you visit whether you're in normal or private browsing mode. Many ISPs share this kind of information with advertising agencies, which will, in turn, use the data to target you with relevant ads.

To hide your internet traffic from surveillance and monitoring, you can use a virtual private network (VPN). VPNs encrypt internet traffic and channel it through a third-party server, which then directs it to the destination. Your ISP will know you're using a VPN, but it won't be able to figure out which websites you're visiting.

Although VPNs protect you against ISP snooping, they sometimes collect and sell your information to other parties. So for absolute privacy, use the Tor browser. Tor encrypts your traffic and bounces it across several computers, called Tor nodes, before reaching its destination. None of the Tor nodes have full information about the source and destination of your internet traffic and can't spy on you. Tor is more private than VPNs, but it's also slower.

Private Browsing Does Not Stop Malware, Viruses

In the aforementioned study by the University of Chicago and Leibniz University, 25 percent of respondents said they believe private browsing protects them against malware and malicious websites.

RECOMMENDED BY OUR EDITORS

Facebook: We Stored Millions of Instagram Passwords in Plain Text

76 Percent of Parents Concerned For Children's Online Safety

But most malware will cause harm after it is installed on your computer, and malicious websites will harm you regardless of your browsing mode. For instance, when you open a phishing email and download a malware-infected attachment while browsing in private mode, you won't be protected (by your browsing mode). Also, private browsing won't protect you against malware already installed on your computer: a keylogger, for example, that silently monitors your keystrokes and sends them to a hacker's server.

To protect yourself against malware, you'll need an antivirus.

An exception to this is malicious extensions—the third-party features you add to your browser. Some hackers hide malware in browser extensions and do things such as steal your credentials or mine cryptocurrencies. Edge, Chrome, and Opera disable extensions by default, which will protect you against malicious browser extensions that might have found their way to your browser. Other browsers won't disable

extensions in private browsing, but it takes only a few clicks to do it manually, and it's considered a good privacy practice.

Private browsing is a very useful and handy tool for a quick surfing session that will not leave traces on your computer. With a few caveats, it will protect your privacy against other people who use your computer and reduce some of the information you reveal about yourself when visiting websites.

But private browsing won't make you anonymous and won't protect you against surveillance and big tech snooping. For that, you'll need true privacy tools.

EXHIBIT 108

LAURIE CLARKE SECURITY 20.07.2019 06:00 AM

Google Chrome's Incognito Mode is way less private than you think

Google Chrome 76 is limiting how you can be tracked in its Incognito Mode. But that doesn't mean you're not being tracked at all

GOOGLE / WIRED

The icon is a detective style hat and glasses, the colour scheme is moody, and many think that entering Google Chrome's Incognito Mode is like slipping under a cloak of invisibility. Yet it turns out that this is hopelessly misguided. Despite the long-known fact that Incognito isn't truly anonymous, new research has re-emphasised that Google and other web browsers are still tracking you in privacy mode, even on the most sensitive of sites.

A forthcoming research paper, set to be published in the journal New Media & Society and first reported on by the *New York Times*, saw researchers scan 22,484 porn websites. They found 93 per cent of them housed trackers sending information to an average of seven third party domains. While this may be startling many people, incognito has always made for an inadequate privacy tool.

“Private modes in web browsers were never designed as a general privacy fix,” says Lukasz Olejnik, independent cybersecurity and privacy advisor, as well as research associate at the Center for Technology and Global Affairs at Oxford University. “In practice, they offer very little.”

The modes are short-term options that can limit what's recorded on one machine – not an all-encompassing way to be private online. The main functionality of incognito mode is not saving cookies or browser history on the hard disc, meaning that private browsing sessions are isolated from normal ones.

Third party tracking is generally achieved by websites storing cookies on a visitor's hard drive. Cookies are generally used to track repeat visits from the same user, and build up a profile that's used to serve ads. In incognito mode, your data is tracked in exactly the same way as normal mode. “The difference is that in ordinary circumstances, trackers are unable to link a "private browsing" session with the "normal session",” says Olejnik. “This means that in principle, after the user closes the browser window no trace should be left.”

But there are of course problems. Notably, third-party sites are able to detect whether site visitors are in private browsing mode, something that Olejnik says is being weaponised against them. It's this capability that allows, for example, news sites with paywalls to block access to visitors with this mode enabled. If you reach your limit of free articles on the *New York Times*, it's still able to recognise you (and stop access) if you click into incognito.

However, most browsers have never really considered this a major privacy flaw. This is why one loophole that allows third party websites to do this – through Filesystem API detection –

has remained in place for so long. The FileSystem API is disabled in Incognito mode, meaning that if a site searches for it and gets an error message, they can determine that a user is in privacy mode. Google has announced the next iteration of its web browser, Chrome 76, will close the loophole. When it's released on July 30, it's probably not going to please publishers.

Read more: How to delete your Google search history and stop tracking

However, despite the loophole being shut, this doesn't mean that Chrome's Incognito Mode will become a better way to browse anonymously. Matthew Forshaw, a lecturer in Data Science at Newcastle University was involved in research that compared the privacy modes of different browsers, and found that a lot of their claims didn't stack up.

This research, conducted back in 2014, uncovered that third party websites were leveraging cookies to identify which users were browsing privately. In normal browsing, cookies are written onto the hard disc itself, whereas in incognito mode, they are held in a device's memory. The research demonstrated that a third party website could remotely instruct someone's browser to write one million cookies, and track how long it took – in a normal browser mode it should take a number of seconds, but when using private mode it's almost instantaneous.

Another means of determining this mode is almost deceptively simple. Though you may be in private mode, there will only be so many people running the same version of your operating system with that version of the browser. From this information alone, trackers can often identify more personally sensitive and identifiable information. Forshaw says internet users can use a programme called Panoptoclick to obtain a 'uniqueness score' – ostensibly telling you how easily identifiable you are as you browse the web. The research project is run by the Electronic Frontier Foundation.

Is your browsing history at least safe from family members or partners who may have access to your computer? Forshaw's research found that someone with access to your machine could discover which websites had been browsed with easily available tools. On the hard disc and in the memory, there were traces of which websites had been visited when in incognito mode.

But is this all of this by design? From its inception, Google's whole business model has been predicated on collecting vast collections of data about its users. To create a truly private browsing option where no data is tracked would run directly counter to the tech giant's raison d'etre. However, Google doesn't claim that incognito is a catch-all security salve. In fact, it highlights that your activity might still be visible to the websites that you visit, your employer or school (if you are accessing content via an institution's internet connection) and your internet service provider.

However, when it comes to third party tracking, Forshaw dismantles the notion that these entities may end up capturing such data 'by accident'. "There's a possibility than one of these trackers makes a decision about what they consider in and out of scope, and that through technical fluke, they end up capturing more information than they intended," he says, "but in general, it's probably very well considered."

Given privacy modes don't guarantee a true layer of anonymity, it's not surprising that they offer no protection higher up the food chain. Your activity will still be available to your internet service provider which can monitor your activity using your public IP address.

There are other options though. If you're looking for a more private online experience, you want to consider a privacy-first web browser. You'll get the most protection by using Tor, which reroutes and encrypts your online activity in multiple layers, but other alternatives such as Brave and DuckDuckGo collect less data than Google's offering.

More great stories from WIRED

🕵 **It's time you ditched Chrome for a privacy-first web browser**

🚕 **London's minicabs have a cunning plan to beat Uber**

🎉 **A vaccine for Alzheimer's is on the verge of reality**

🤦 **Reddit's 'Am I the Asshole' is your new guilty pleasure**

📧 **Get the best tech deals and gadget news in your inbox**

TOPICS PRIVACY SECURITY TECHNOLOGY GOOGLE

EXHIBIT 109

TECHNOLOGY (/TOPICS/TOPIC/CATEGORIES/TECHNOLOGY.HTML)

JASON GROW FOR AL JAZEERA AMERICA

Ask the Decoder: How private is private browsing, really?

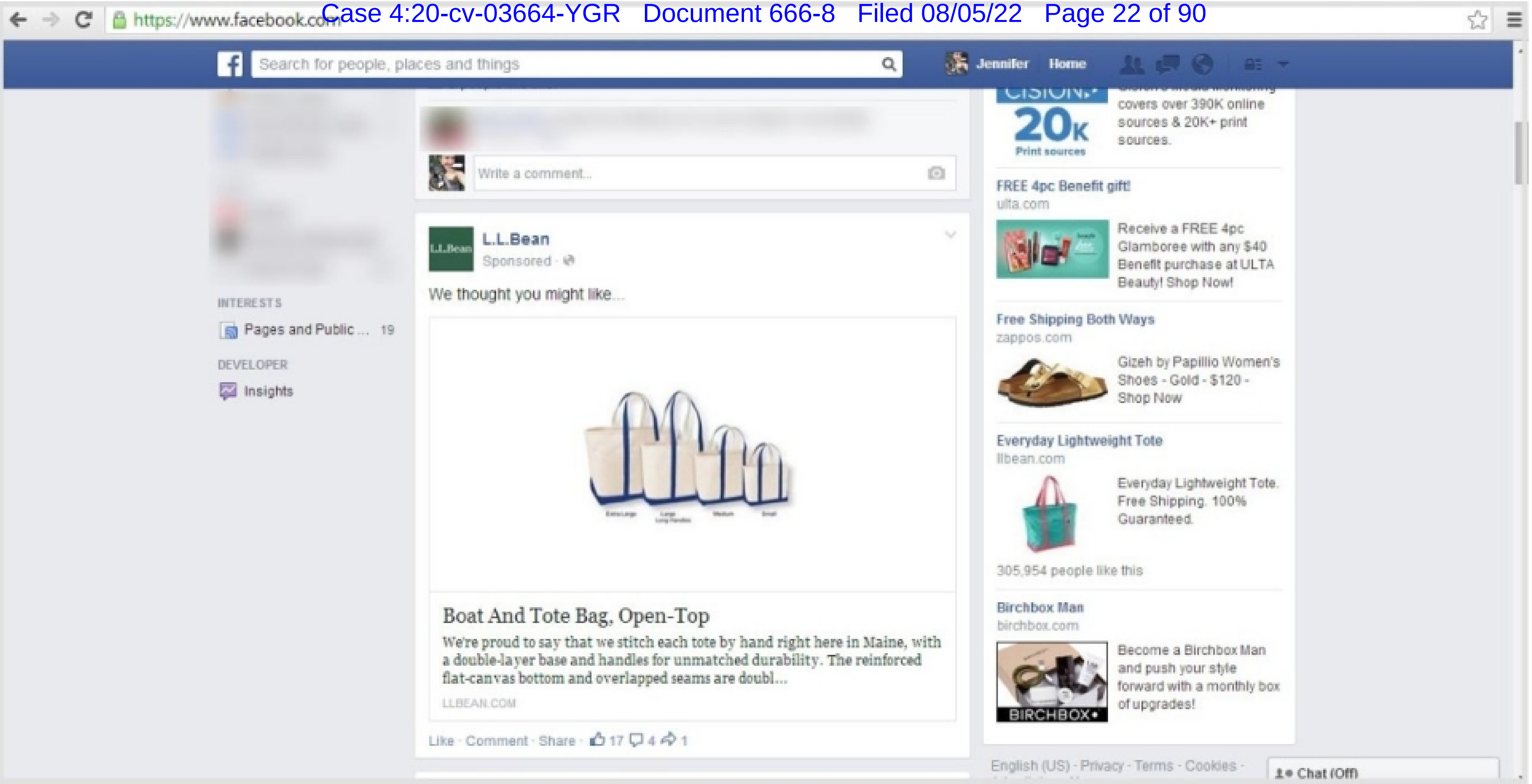
When incognito is like hiding in plain sight

September 24, 2014 1:00AM ET

by **Sara M. Watson (/profiles/w/sara-m-watson.html)** - @smwat (http://www.twitter.com/smwat)

Editor's Note: This is the second installment of The Decoder (http://america.aljazeera.com/articles/2014/9/15/sara-m-watson-bio.html), a column that's part of the Living with Data (http://america.aljazeera.com/topics/topic/issue/living-with-data.html) series exploring how our online data is tracked, collected and used. Do you have questions about how your personal data is being used? Curious to learn more about your daily encounters with algorithms? Email The Decoder at thedecoder@aljazeera.net (mailto:thedecoder@aljazeera.net) or submit your question via the form here (http://america.aljazeera.com/multimedia/2014/9/submit-to-decoder.html). Screen shots and links are helpful clues!

My close friend Jen and I were working together one day this summer. (Actually, it was an excuse to hang out with her new puppy all day.) Taking a break, she opened Facebook in a new tab. She turned her laptop toward me, freaked out that all the ads she saw were for either specific items she had looked at or websites she recently visited. She was being bombarded by retargeted ads similar to ones we explored last week (http://america.aljazeera.com/articles/2014/9/16/the-decoder-stalkedbysocks.html).



L.L.Bean
Sponsored ·

We thought you might like...

Boat And Tote Bag, Open-Top

We're proud to say that we stitch each tote by hand right here in Maine, with a double-layer base and handles for unmatched durability. The reinforced flat-canvas bottom and overlapped seams are doubl...

LLBEAN.COM

CISION 20K Print sources

covers over 390K online sources & 20K+ print sources.

FREE 4pc Benefit gift!
ulta.com
Receive a FREE 4pc Glamboree with any $40 Benefit purchase at ULTA Beauty! Shop Now!

Free Shipping Both Ways
zappos.com
Gizeh by Papillio Women's Shoes - Gold - $120 - Shop Now

Everyday Lightweight Tote
llbean.com
Everyday Lightweight Tote. Free Shipping. 100% Guaranteed.
305,954 people like this

Birchbox Man
birchbox.com
Become a Birchbox Man and push your style forward with a monthly box of upgrades!

Remember to buy all of these things while you are incognito browsing. Screenshot from Chrome, Jen Hudon

But the surprising thing for Jen wasn't the ads themselves but that they were showing up while browsing in incognito mode in Chrome. She didn't expect to see that kind of personalization while browsing in what she thought was a private setting, deleting her browsing history along the way.

We wondered, how private is private browsing, really? She recounted the incident:

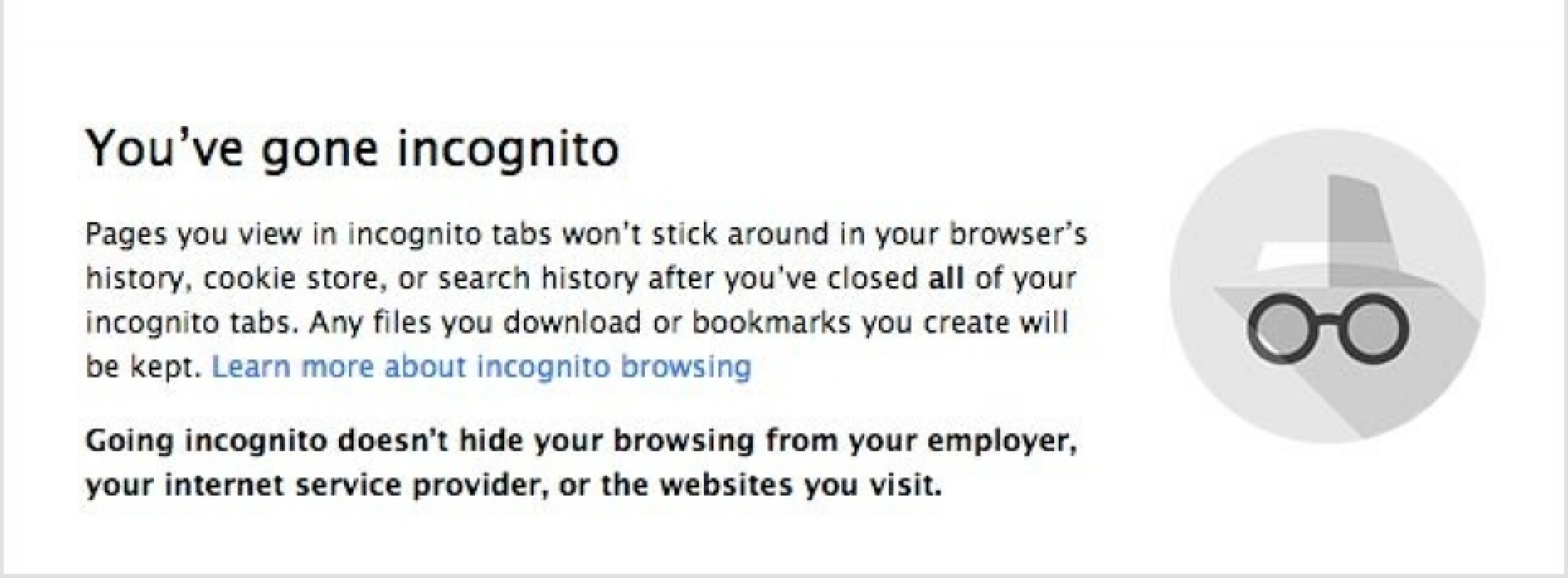
> *Hey, Decoder. The piece about socks last week reminded me that I'm still trying to understand why certain brands and products are following me around while I'm incognito browsing. I thought my browser couldn't track my site visits as long as I was in incognito mode, but looking at my Facebook feed is like looking at my website history. Here's a screenshot I grabbed this summer. I had Bean boat bags, Birkenstocks and Benefit products on different incognito tabs, and each exact product and site showed up as a sponsored ad on Facebook. I keep my browser open a lot of the time — maybe that's why? Not all my tabs were closed after browsing. The next time I opened a new tab, I noticed a message from Google about incognito features for the first time. Can you help decode this?*
>
> — Jen Hudon, Natick, Massachusetts

Expectations of incognito

I followed up with Jen and she explained that she uses private browsing all the time on her work computer because it feels safer to automatically get rid of cookies and browsing history. Months later, she's still using it, even though she's not sure it's doing much to control what is collected from her browsing.

Jen was surprised by the retargeted ads because she knew they were based on cookies and history, but she thought she wasn't leaving those trails behind her. Upon further inspection she realized that cookies are deleted only after she closes out all the incognito windows. Like a lot of us, Jen doesn't often shut down her computer completely, and she keeps a few regular tabs open most of the time. It seems like incognito mode wasn't really designed to protect that kind of browsing behavior.

The real disconnect for Jen was that private browsing mode clears your browsing history only from your local machine, whether its your computer or your phone. Not from anywhere else.



You've gone incognito

Pages you view in incognito tabs won't stick around in your browser's history, cookie store, or search history after you've closed **all** of your incognito tabs. Any files you download or bookmarks you create will be kept. Learn more about incognito browsing

Going incognito doesn't hide your browsing from your employer, your internet service provider, or the websites you visit.

What incognito doesn't do, in bold. Screenshot from Chrome, Jen Hudon

Parsing 'private' browsing

All the major browsers have some form of private browsing: Chrome (https://support.google.com/chrome/answer/95464?hl=en), Firefox (https://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info), Safari (http://support.apple.com/kb/PH17168), Internet Explorer (http://windows.microsoft.com/en-us/internet-explorer/products/ie-9/features/in-private) and Opera (http://help.opera.com/Windows/12.10/en/private.html).

Here's how Google describes (https://support.google.com/chrome/answer/95464?hl=en) the incognito browsing function: "If you don't want Google Chrome to save a record of what you visit and download, you can browse the Web in incognito mode." You can use this mode on desktop and mobile Chrome browsers. Google describes incognito mode in cute animated movie (http://youtu.be/bu5b_jYWVcQ) as a way to keep surprises (such as an anniversary party) secret from people who share your computer.

But private browsing doesn't mask your activity from internet service providers, search engines or websites that you visit. Sites that you go to still receive information about you like location, browser information and IP address. Cookies are still dropped and are cleared only when you close the window. IP addresses detailing the direction of traffic still travel over your Internet service provider's network. And it doesn't hide documents you download.

Depending on what information you are trying to protect and from whom, private browsing might not be the right solution.

Browsing with Tor (https://www.eff.org/deeplinks/2014/06/why-you-should-use-tor) can help mask your IP address, as can using a VPN (http://lifehacker.com/5940565/why-you-should-start-using-a-vpn-and-how-to-choose-the-best-one-for-your-needs). The Guardian Project's (https://guardianproject.info) Orbot (https://guardianproject.info/apps/orbot/) mobile browser uses Tor as well. But Tor works only when enough people are also using it. Alternative search providers like Duck Duck Go (http://privatebrowsingmyths.com) compete with Google by promising not to save your searches at all.

Mobile private browsing is especially tricky, suggests Nathan Freitas (https://twitter.com/n8fr8) of the Guardian Project. On our phones, browsing data is stored all in one place and is often shared across apps. It's difficult to be sure, even after a private browsing session is closed, that other details aren't discoverable on the device. Mobile privacy is starting to get better, with iOS 8 allowing users to choose Duck Duck Go (http://www.fastcolabs.com/3035849/starting-today-your-iphone-can-ditch-google-for-duckduckgos-private-search) as their default search engine.

There are plenty of reasons you might want to keep your browsing from others. Maybe you're looking for birthday gifts. Maybe you just want to window-shop in peace without socks stalking you (http://america.aljazeera.com/articles/2014/9/16/the-decoder-stalkedbysocks.html). Maybe you want to entertain your hypochondriac WebMD searches without worrying about future embarrassment or contributing to flu trends research. Maybe you are using it for the most obvious unmentionable, porn. Or maybe you are an activist in a war-torn country at risk of physical harm.

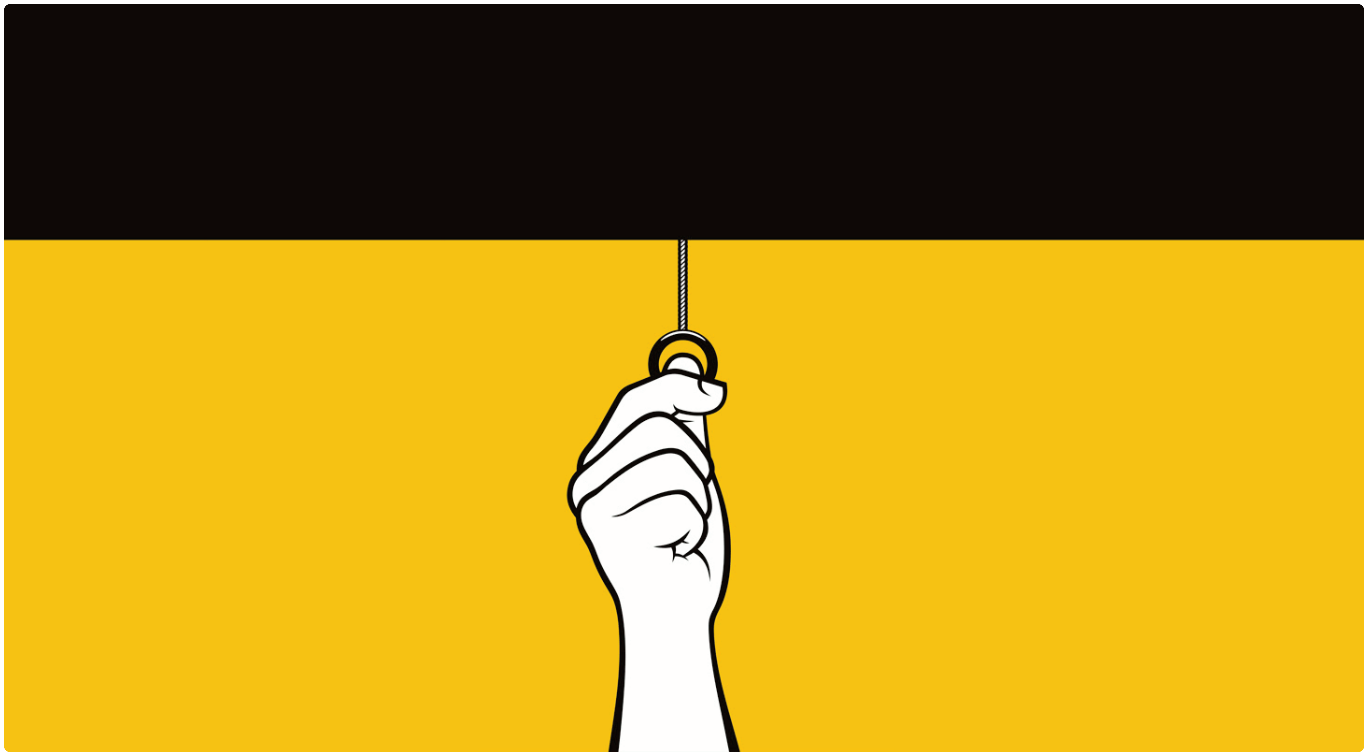
No matter what you are trying to do, it's important to know what "private" really means in private browsing.

Do you have questions about how your personal data is being used? Curious to learn more about your daily encounters with algorithms? Email The Decoder at thedecoder@aljazeera.net (mailto:thedecoder@aljazeera.net) or submit your question via the form here (http://america.aljazeera.com/multimedia/2014/9/submit-to-decoder.html). Screen shots and links are helpful clues!

EXHIBIT 110

How Anonymous Is DuckDuckGo?

FILED UNDER DUCKDUCKGO Q&A



If you're unfamiliar with DuckDuckGo, we are an Internet privacy company that empowers you to seamlessly take control of your personal information online, without any tradeoffs. We operate a search engine alternative to Google at https://duckduckgo.com, and offer additional apps and extensions to protect you from Google, Facebook and other trackers, no matter where you go on the Internet.

DuckDuckGo search is completely anonymous, in line with our strict privacy policy. Each time you search on DuckDuckGo, you have a blank search history, as if you've never been there before.

We simply don't store anything that can tie searches to you personally. In fact, we don't even store anything that could even tie anonymous searches together into an anonymous search *history*, which has been shown in some cases to be able to be de-anonymized (like if you searched for personal information about yourself). That's also why we can't tell you for sure how many people use DuckDuckGo, because if we counted, our users wouldn't necessarily be anonymous. Yes, we take privacy that seriously.

While DuckDuckGo is completely anonymous, Google is of course not. In fact, quite the opposite. On Google, your searches are tracked, mined, and packaged up into a data profile for advertisers to follow you around the Internet through those intrusive, annoying, and ever-present banner ads, via Google's massive ad networks , embedded across millions of sites and apps.

Unfortunately, people think that they can make searching Google and browsing the rest of the web anonymous by using Chrome's so-called "Incognito" mode (also known as Private Browsing mode) or its "Do Not Track" browser setting. Sadly, neither of these mechanisms protect you from Google search tracking or its trackers on other websites. We believe it is important to expand a bit on these myths so that you don't have a false sense of security if you choose to utilize those methods.

The Myth of Incognito Mode

A lot of people are shocked to learn that websites can still track you even in Chrome's "Incognito" mode.

The truth is that Chrome's Incognito mode only prevents your browser history from being recorded on your local device and does not offer any additional protection such as preventing the websites you visit from collecting your information (e.g., your searches on a search engine). Check out the fine print.

It is simply a myth that Incognito mode protects your online privacy in any significant way; it is really more of an offline protector. You can easily still be uniquely identified and tracked while using Incognito mode through “browser fingerprinting.” Just as each person has a unique fingerprint, so does every browser. Websites can look at your IP address, version numbers of your browser, the plugins it uses, and dozens of other points of browser information to create a unique ID — a *browser fingerprint* —that can then be used to track you.

That is, while in Incognito mode, Google is still tracking your searches, and can use them to send intrusive ads at you across the Web on the millions of sites and apps that run Google ads. Sure, your search or browser history won’t be on your computer, but Google still knows it. And when you get served an ad based on that "incognito" search you did recently (like, let’s say that surprise vacation you were planning), it’s not so private anymore. On the other hand, DuckDuckGo doesn’t track your search history at all, regardless of whether you’re “incognito” or not.

We surveyed 5,710 random Americans about Incognito mode to understand what people know about and how they use this common feature. 65% of respondents reported feeling “surprised”, “misled,” “confused,” or “vulnerable” upon learning about the limitations of Incognito mode.

Note that some browsers other than Google’s Chrome browser do have private browsing modes that do more to protect you online. Nevertheless, we suggest adding our browser extension to Chrome or other browsers as it blocks more web trackers as you surf the web, helps you use more encryption, and reveals the privacy practices of every website you visit.

The Myth of Do Not Track

In trying to escape Facebook and Google web tracking, you might have turned on the “Do Not Track” browser setting. Unfortunately, it's voluntary and Facebook and Google do not respect it.

Without regulatory measures, the “Do Not Track” setting as it currently stands, is a voluntary setting that hardly anyone respects (including Facebook and Google) which makes it not only ineffective, but worse, misleads people into feeling a false sense of privacy.

Let’s Make the Internet More Private

Our mission is to set a new standard of trust online through the privacy tools DuckDuckGo provides – our anonymous search engine at https://duckduckgo.com and our apps and extensions that protect your privacy while browsing the web.

Despite increased awareness of privacy issues and actions people can take, there are sadly still many people putting their privacy at risk, or, browsing with a false sense of privacy. This happens for a variety of reasons, including practices such as relying solely on Chrome’s “Incognito” mode and Do Not Track setting, as we’ve detailed here.

To help correct these misconceptions and reach more people, we’re also trying to educate users through our blog, social media and a privacy “crash course” newsletter.

The Internet shouldn't feel so creepy and getting the privacy you deserve online should be as simple as closing the blinds.

For more privacy advice, follow us on Twitter & get our privacy crash course.

EXHIBIT 111

Privacy Matters: Don't Let Google Chrome's 'Incognito Mode' Fool You

Credit: Valentin Wolf / Shutterstock

Google Chrome is one of the most popular browsers in the world. It comes pre-installed on all Android devices and is one of the most commonly used browsers on both Macs and iOS devices. And you've probably used the popular Chrome feature called Incognito Mode, which is similar to Apple's Private Browsing Mode.

Many users believe Incognito Mode will keep them safe while browsing the internet. However, Google even admits that Incognito Mode is *not* that protective.

What Happens When You Browse Incognito?

- Chrome won't save your browsing history, cookies, site data, or information entered in forms.
- Files that you download and bookmarks that you create will be saved.
- Your activity *isn't* hidden from the **websites you visit**, your **employer** or **school**, or your **internet service provider**.
- If you sign into an account to use a web service, like Gmail, your browsing activity might be saved on the sites that recognize that account.

What Is the Purpose of Incognito Mode?

Incognito Mode prevents your computer from storing cookies and surfing history, but it doesn't prevent websites from storing your information (and Google runs some of the most commonly visited websites).

Reportedly, 23 of the top 100 sites visited worldwide are owned by Google. So while using Chrome, Google will still share your information with itself, even when Incognito Mode is on.

If you sign into any of your Google accounts while using Incognito Mode, they'll continue to track what you do on those web sites. One option to prevent yourself from being tracked is to make sure you're logged out of all of your Google accounts before going into Incognito Mode.

What Can You Do to Protect Yourself?

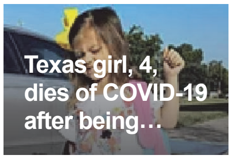
The easiest thing you can do, is to choose websites that don't collect your personal data. Even choosing another browser isn't going to fix the problem, however there are still some great tools you can use.

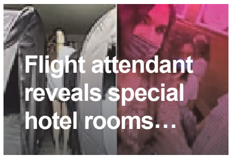
Blocking cookies will prevent websites from storing small pieces of information on your computer that can be used to track you.

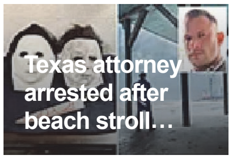
You also can adjust settings within your browser to ask websites not to track you. Make sure you're using secure websites, try to stay away from data-collecting websites, and if possible, use a VPN.

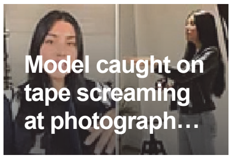
EXHIBIT 112

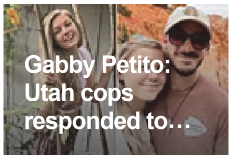
NEW YORK POST

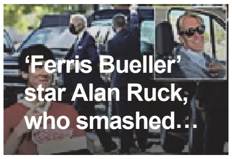

Texas girl, 4, dies of COVID-19 after being…


Flight attendant reveals special hotel rooms…


Texas attorney arrested after beach stroll…


Model caught on tape screaming at photograph…


Gabby Petito: Utah cops responded to…

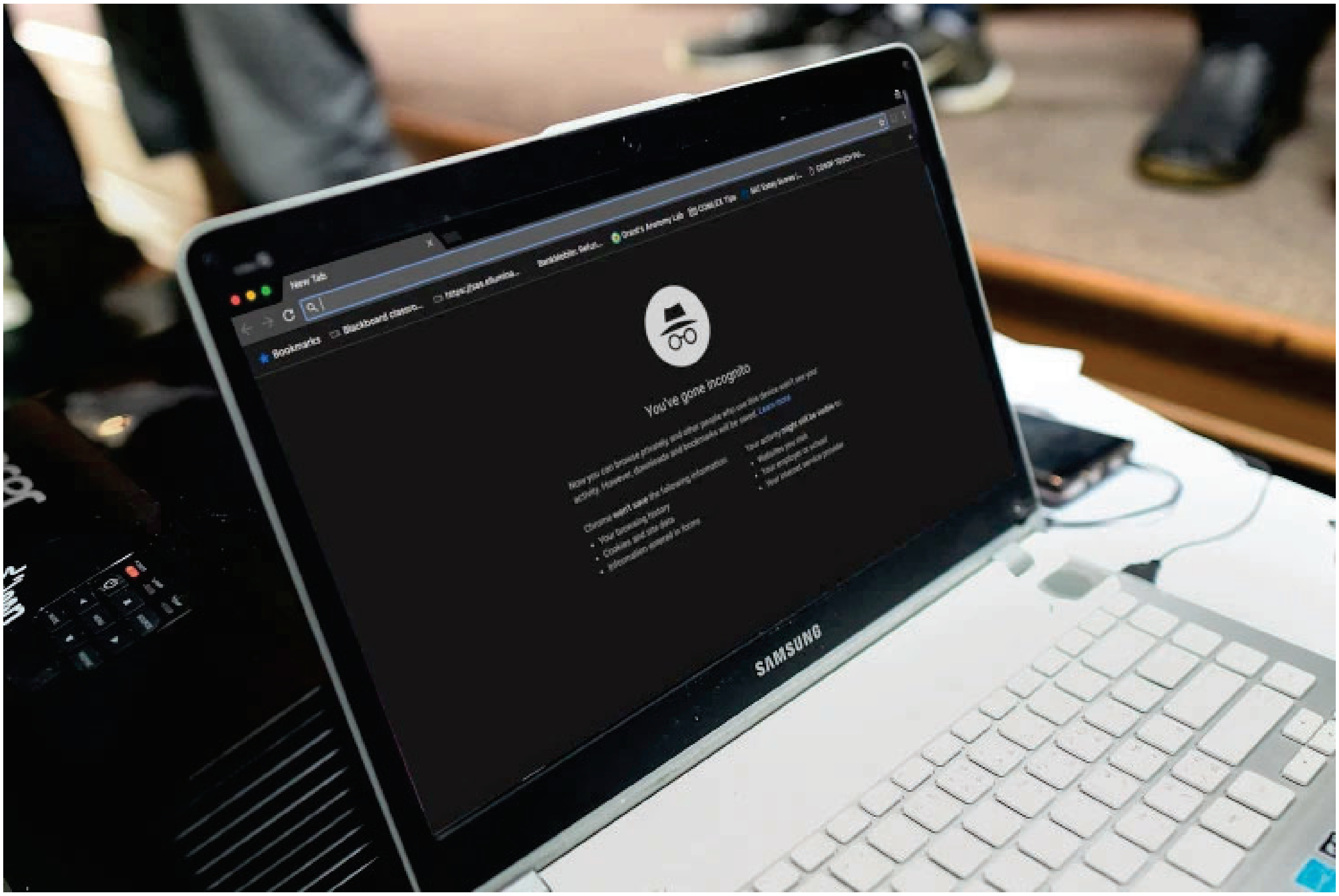

'Ferris Bueller' star Alan Ruck, who smashed…

TECH

Google's incognito mode isn't as private as you thought

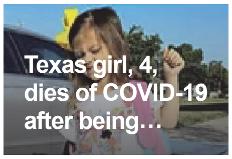
By Sean Keach, The Sun

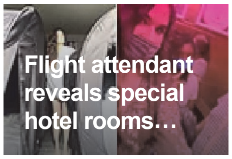
August 22, 2018 | 12:25pm | Updated

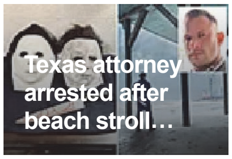


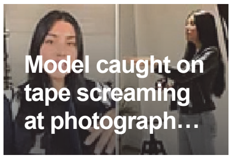
NEW YORK POST

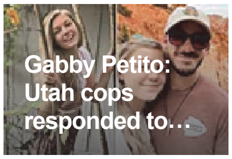
LOG IN

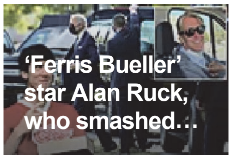












'Ring of Fire' hit with 70 earthquakes in just 48 hours

Facebook to rate users on trustworthiness

World's biggest plane set for the skies

NASA admits Opportunity rover could be lose forever

Google's Incognito Mode is a great way to hide your online antics — but there's a big hole that could leave you exposed.

A new study from Vanderbilt University reveals a sneaky way Google can see exactly what you've been looking at online.

The study investigated how Google collects info from across devices (like Android or Chromebooks) and services (like Google, YouTube and the Chrome web browser).

And it revealed something very surprising about Incognito Mode.

It emerged that Google can still record the websites you browse while in Incognito Mode on the Chrome browser and link them to your identity.

This will come as a surprise to some users who thought the special setting protected them.

Incognito Mode is a setting on Chrome that prevents your web history from being stored.

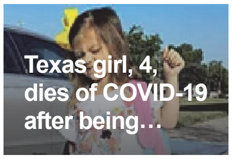
It also won't store cookies — small files about you — that are linked to your identity.

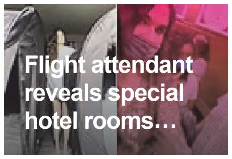
If you're logged into Google, much of what you do online can be traced back to your personal account.

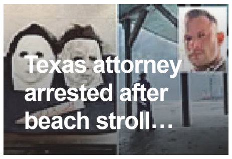
But if you switch Incognito Mode on, you'll only receive "anonymous" cookies and Google won't be able to link your identity to your browsing habits.

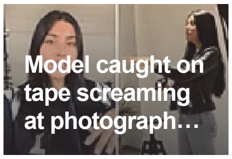
NEW YORK POST

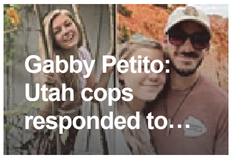
LOG IN

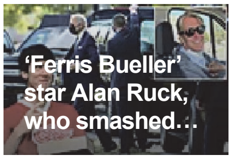












Incognito Mode — and link it to your Google identity.

This works by taking the previously anonymous cookies and then associating them with your Google account.

The only way to get around this would be to only log into your Google account after you've left Incognito Mode.

"While such data is collected with user-anonymous identifiers, Google has the ability to connect this collected information with a user's personal credentials stored in their Google Account," the study explained.

Douglas Schmidt, a professor of computer science who authored the study, said the loophole is "not well understood by consumers."

"If you read the fine print on 'incognito' mode, it brings up a whole lot of disclaimers," said Schmidt, as quoted in a report by AdAge.

He said Google collects "all the information necessary" to connect your browsing to your identity.

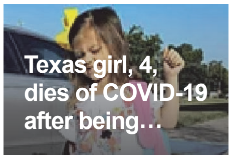
"It would give them a relative advantage to anyone else who can't do that correlation," he added.

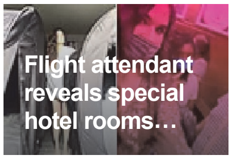
The news comes just days after Google was exposed for spying on your real-world movements, even if you have its Location History setting turned off.

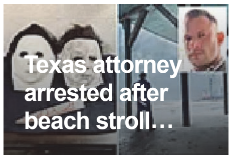
To stop Google tracking your location, you can follow our handy guide.

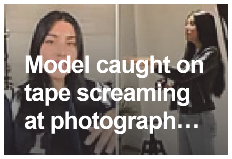
As far as Incognito Mode goes, it's also worth mentioning that while the setting stops Google Chrome from saving your browsing habits on your own computer, it won't protect you from outsiders seeing what you do online.

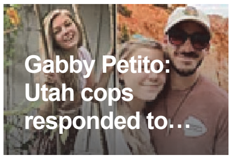
Anyone on your Wi-Fi network could potentially use special spy software to view what you're browsing, regardless of Incognito Mode.

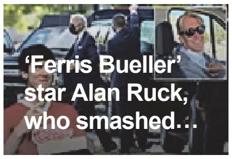

Texas girl, 4, dies of COVID-19 after being…


Flight attendant reveals special hotel rooms…


Texas attorney arrested after beach stroll…


Model caught on tape screaming at photograph…


Gabby Petito: Utah cops responded to…


'Ferris Bueller' star Alan Ruck, who smashed…

That means the police can also get access to what you view in Incognito Mode, simply by requesting that information from your internet provider.

The websites you're using will also be able to track that you're on their page, too.

For instance, Google will know where you're browsing from and what you're looking at.

And if you log into a website, they'll also be able to keep track of information about you.

So when you log into Facebook in Incognito Mode, details about what you do on the site will be recorded — just the same as if you were using it in a normal web browser.

The key point is that Incognito Mode is not a great method of ensuring privacy, because it's still very easy to track what you're doing online.

It's only really useful for keeping websites out of your browsing history or logging into a single website on multiple accounts in the same web browser.

FILED UNDER DIGITAL PRIVACY , GOOGLE , 8/22/18

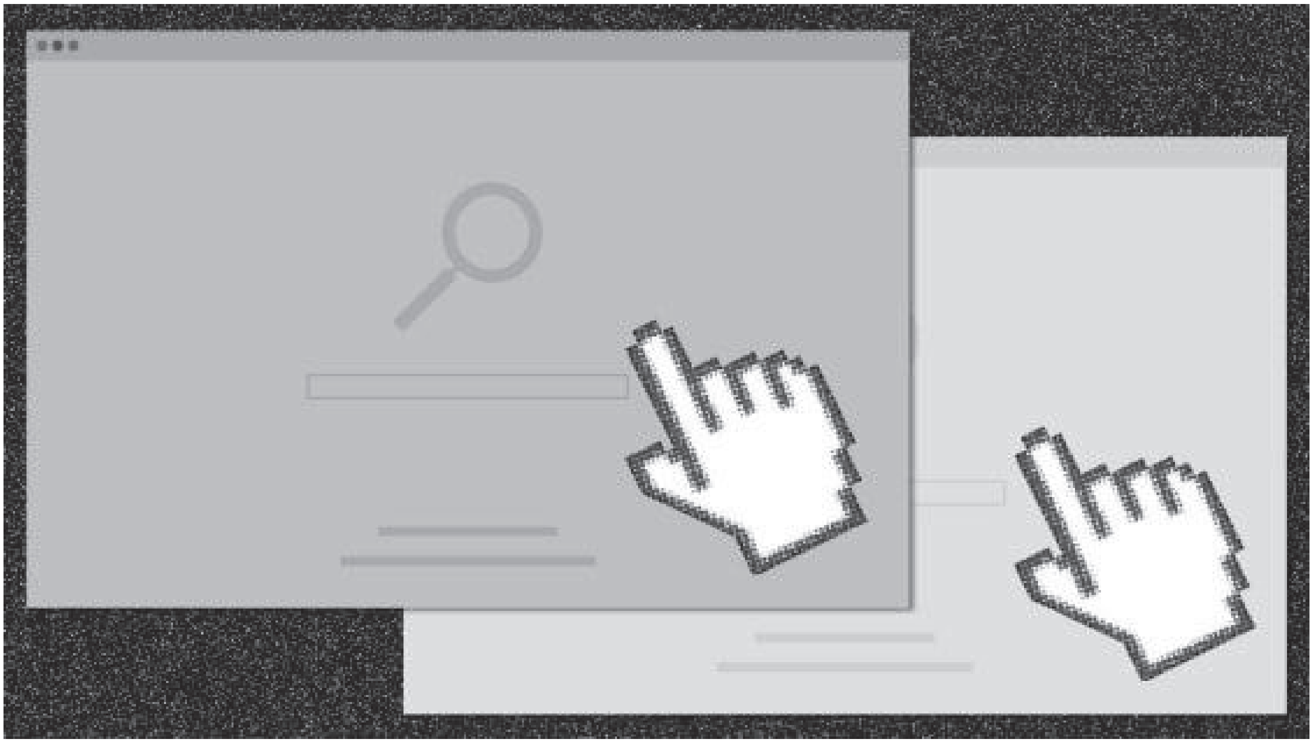
READ NEXT Dating apps are ever-expanding pits of desirous despair

EXHIBIT 113

04-12-19

Incognito mode won't keep your browsing private. Do this instead

Browser compartmentalization can help you escape the clutches of the data gathering machine.



[Illustrations: janjf93/Pixabay]

MORE LIKE THIS

- Luna 2.0 is about to launch: What you need to know after TerraUSD's spectacular collapse
- Bye, Zoom: This smart new app is the future of online meetings
- What we know about Javier Olivan, Facebook-parent Meta's new COO

BY MICHAEL GROTHAUS

8 MINUTE READ

This story is part of The Privacy Divide, a series that explores the misconceptions, disparities, and paradoxes that have developed around our privacy and its broader impacts on society. Read the series here.

The big tech giants, online advertising companies, and data brokers use a ton of tricks to track you around the web. These include things like cookies, location and device logging, fingerprinting, and even share buttons, the last of which make it very easy for companies like Facebook and Google to see what you do online, even on third-party websites.

Of course, today's users aren't blind to much of this tracking. And most people who are aware of it will take (somewhat predictable) steps to do what they think will hide their online activity from tech companies.

One of the most common techniques people think can help hide their activity is the use of an "incognito" mode in a browser. This opens a secure browsing window where third-party cookies are blocked and browsing history is paused.

SORRY, NO

The problem with incognito modes is they provide a false sense of security.

Despite what most people assume, incognito modes are primarily built to block traces of your online activity being left on your computer–not the web. Just because you are using incognito mode, that doesn't mean your ISP and sites like Google, Facebook, and Amazon can't track your activity.

This is especially true if you log into any of these sites in your browser after you're in an incognito window–the companies can still see everything you do. And it's the same for any other site you need to log in to. So remember that if you're logged in to a website, no matter if you are using incognito mode, or even a VPN, the website's owners can see exactly what you are doing.

For the people who recognize the limits of incognito mode, they'll generally then use browser extensions to help block more information being sent back to tech companies. These usually involve script, cookie, and ad blockers. The problem with this is that many websites rely on those same technologies to work right–again, this is especially true of websites you need to log into, like banks, social media sites, and shopping sites.

Usually, the sites that require scripts and cookies to work will show you a notification telling you that you need to whitelist them if you want to use the site properly. Whitelisting them gives you back the site's functionality, but then you lose the privacy protections you were seeking in the first place, because those sites will once again place tracking cookies on your computer to follow your online footsteps. So what is a privacy-conscious person supposed to do?

BROWSER COMPARTMENTALIZATION

Browser compartmentalization is a privacy technique that is finally gaining mainstream attention. The technique sees users using two or even three browsers on the same computer. However, instead of switching between browsers at random, users of browser compartmentalization dedicate one browser to one type of internet activity, and another browser to another type of internet activity.

Here's how it works:

Users will use one browser for any and all websites they need to log in to. This browser is the one on which they'll access their social media, banks, and shopping sites.

The big catch here is that users will never use this browser to search the web or randomly browse the internet. This browser is only used for bookmarked sites you need to log in to. Let's call this your "accounts" browser.

Users will then use a second browser for all their web searching and random browsing. On this browser, a user will never log into any website–ever. They will never use this browser to personally identify themselves in any way, period. We'll call this your "everyday" browser.

By splitting up your web activity between two browsers, you'll obtain the utmost privacy and anonymity possible without sacrificing convenience or the ease of use of the websites you need to log in to. That's because the majority of your web usage will be done in your "everyday" browser, which, by never logging into any website, will make it extremely hard for data firms to identify you and track your activities–especially if you fit your "everyday" browser out with some hardcore privacy extensions. You can go all out with your privacy settings on your "everyday browser": Block all cookies, scripts, and trackers, and always use in it incognito mode. That's because you won't be logging into any sites that require cookies or scripts to be enabled to work.

Related: How the tragic death of Do Not Track ruined the web for everyone

A word of warning: This approach won't completely protect your privacy. Your ISP and other companies may still be able to see which sites you are visiting. To completely obscure your traffic, you'll need to also use a VPN.

For websites that do require those technologies to work, like social media sites and banking sites, you'll use your "accounts" browser.

WHY BROWSER COMPARTMENTALIZATION WORKS

The reason browser compartmentalization works is because web browsers are, for the most part, walled gardens. They don't share cookies between them, nor other identifiable items like browser history or bookmarks. Thus, when Google or Facebook places a cookie tracker on your "accounts" browser when you log in to their sites so they can track you around the web, this cookie they've put on your computer is only accessible through that browser, not any other browser on your computer.

SETTING UP YOUR "ACCOUNTS" BROWSER

When configuring your browser compartmentalization setup on your computer, you'll want to decide which browser you'll use as your "accounts" browser, and which one you'll use for your "everyday" browser. Since your "everyday" browser will be the one you use most often to browse the web, I recommend you use a privacy-focused browser that supports a ton of extensions and add-ons, like Firefox or Brave.

For your "accounts" browser, I still recommend you use a privacy-focused browser, but one that doesn't require a lot of add-ons or extensions. Remember, you're going to want to have your "accounts" browser set up to accept some cookies and scripts so you can log in to the websites you need.

That's why on a Mac I recommend using Apple's Safari as your "accounts" browser. It's got decent privacy protections built in, yet ones that won't break websites you need to log in to. As for a PC, good "accounts" browser options include Microsoft's Edge, Firefox, and Brave (the latter two are also good options on the Mac). As for Chrome: It's made by Google, whose sole aim is to know everything you do online, so it's probably best to stay away from Chrome if you value your privacy.

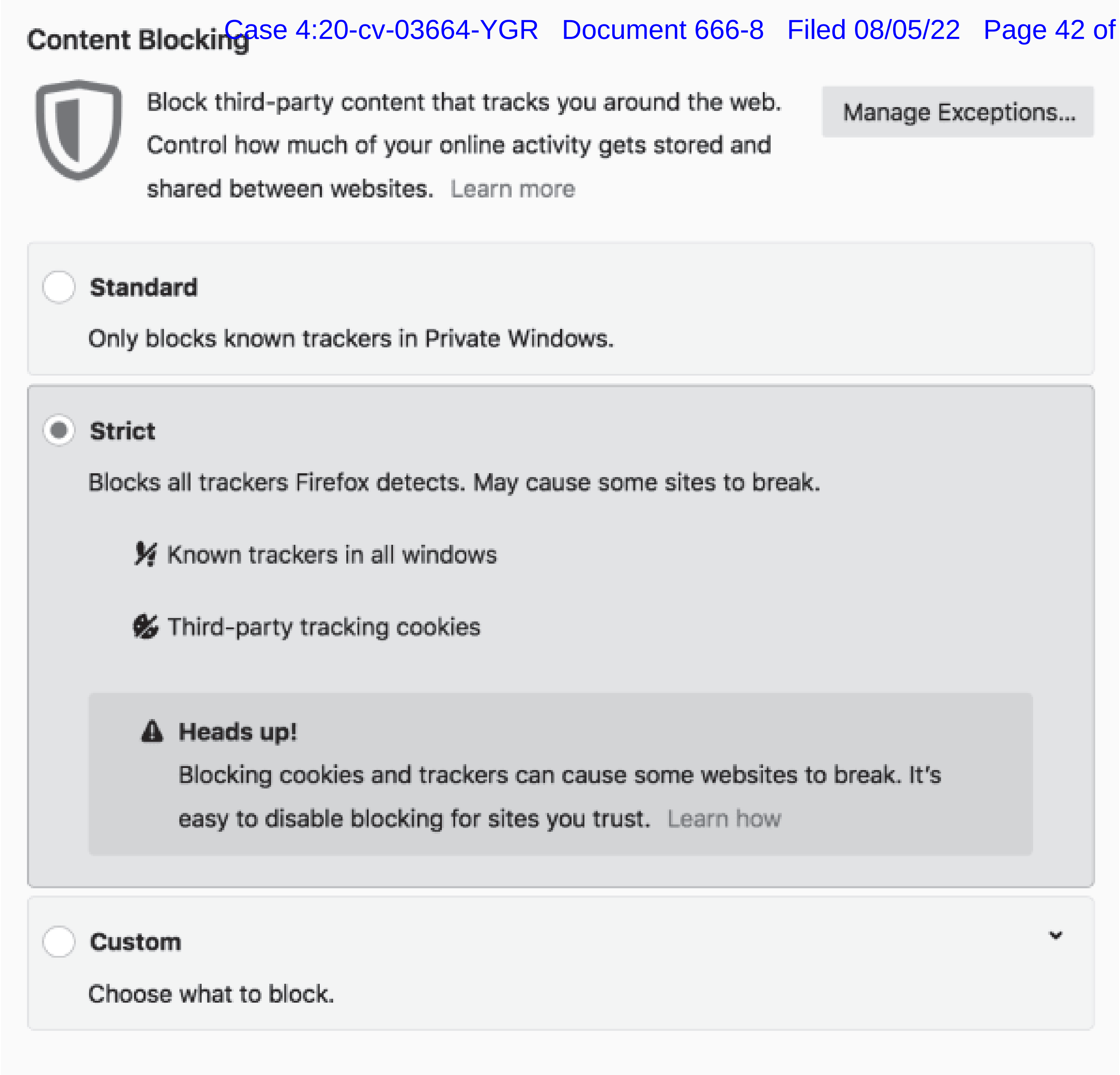
Once you've chosen your "accounts" browser, bookmark every site you use that you log in to: Google, Facebook, your bank accounts, Netflix, airline accounts, utility accounts, Amazon, dating sites, etc. Bookmark them (the toolbar is best for easy access) and access those sites only by clicking on your bookmarks.

Remember: Do not do web searches in this browser. That's what your "everyday" browser is for. By not searching in this browser nor using it to browse the web, you'll greatly limit the online activity the websites you do need to log in to can see. But just in case you forget this and do accidentally perform a search, make sure you change the default search engine in your "accounts" browser to DuckDuckGo, the privacy-focused search engine that doesn't track you.

After you've done this, congratulations, your "accounts" browser is now set up.

SETTING UP YOUR "EVERYDAY" BROWSER

The next step is to set up your "everyday" browser. Remember, this is the browser you will use to search and browse the web, so it's the one you'll be using most of the time. There are plenty of great browsers to use as your "everyday" browser, but I recommend Firefox because it offers so many built-in security and privacy protections, and even more through extensions. This makes it one of the most secure browsers you can use if set up properly. Other viable options include browsers like Brave and the Tor browser.



Content Blocking

Block third-party content that tracks you around the web. Control how much of your online activity gets stored and shared between websites. Learn more

Manage Exceptions...

○ **Standard**

Only blocks known trackers in Private Windows.

● **Strict**

Blocks all trackers Firefox detects. May cause some sites to break.

Known trackers in all windows

Third-party tracking cookies

Heads up!
Blocking cookies and trackers can cause some websites to break. It's easy to disable blocking for sites you trust. Learn how

○ **Custom**

Choose what to block.

In your "everyday" Firefox browser, set your content blocking settings to "strict."

Once you've downloaded Firefox, you will want to do the following:

Do not bookmark any sites you need to log in to, and never log in to those sites on this browser. Remember that you have your "accounts" browser for that.

Go into Firefox's preferences (Firefox > Preferences) and in the General tab click "Make Default" to make Firefox your default browser. By doing this, you can ensure any links you click on in an email will open your "everyday" browser by default.

Still in Firefox's preferences, click on "Privacy and Security." Under "Content Blocking" choose "strict." This will block known trackers and all third-party cookies.

Under "History," check the box labeled, "Always use private browsing mode." This is Firefox's version of incognito mode. Enabling this will ensure your web history is never saved (and thus can never be accessed by a website you visit).

Next, you'll want to download three extensions. The first is uBlock Origin. This extension will block the most intrusive ad trackers and malware.

Now, install the HTTPS Everywhere extension. This extension is made by the Electronic Frontier Foundation, and it forces your browser to request and use the encrypted version of websites, which mean it's harder for your ISP to track what you do on those sites.

Finally, download the Cookie AutoDelete extension. This will automatically delete any cookies, first-party or third-party, that were downloaded during your last browsing session. This ensures that each time you begin a browsing session, no cookies from the last session remain, which makes it almost impossible for sites to track you between browsing sessions.

Once you've done this, your "everyday" browser is now set up. From here on out, all you need to do is remember to keep your online activity compartmentalized between these two browsers. If you need to log in to a site, it's your "accounts" browser you want to go to. If you just want to search or browse the web in relative privacy, simply launch your "everyday" browser.

Remember that browser compartmentalization isn't a perfect privacy method. However, by using browser compartmentalization, you'll make it much harder for the biggest tech companies and data brokers to identify your online activities and track you around the web.

ABOUT THE AUTHOR

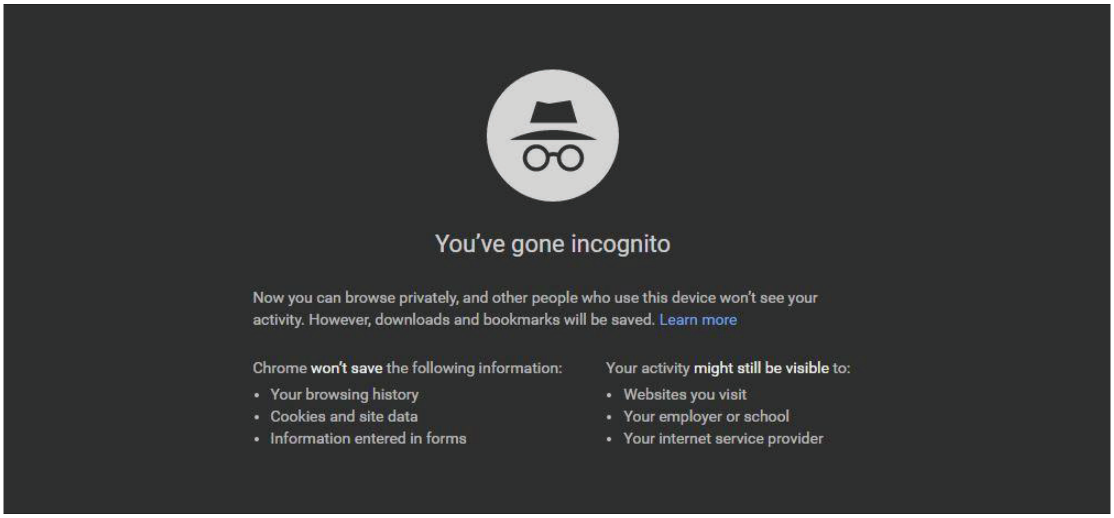
Michael Grothaus is a novelist, journalist, and former screenwriter. His debut novel EPIPHANY JONES is out now from Orenda Books. You can read more about him at MichaelGrothaus.com More

EXHIBIT 114

Privacy Guy Follow

Nov 22, 2017 · 3 min read · Listen

Save



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome **won't save** the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity **might still be visible** to:

- Websites you visit
- Your employer or school
- Your internet service provider

Chrome's Incognito Mode Isn't Private…So What's The Point?

Incognito Mode in Google Chrome, despite its name, isn't really "incognito" at all. The Independent published this article on Tuesday explaining that "incognito" misleads users into thinking their data is protected.

What Does Incognito Mode Do?

Using Incognito Mode, Chrome **won't save** the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

When users open an incognito window, Google discloses: Your activity **might still be visible** to:

- Websites you visit
- Your employer or school
- Your internet service provider

Darin Fisher, Chrome developer, recommends using incognito mode for "avoiding cookies, hiding activities from people who may have access to your computer, such as a loved one you're buying a present for, and protecting yourself against potentially dodgy websites." Incognito mode is essentially the same as clearing your browser history in Chrome.

Why Doesn't Private Browsing Work?

When you use a browser normally, the web browser stores data about your browsing history. If you go to a website, the browser logs that information, stores cookies, and stores form data for autocomplete.

In this transaction, the website is also communicating with your computer and your browser. It collects information, like your IP address and type of device you're using.

Private browsing tells your browser not to record information, but it can't control what information is gathered and stored on other websites' servers. Your history, while invisible on your computer, is probably still available somewhere else.

Private Browser > "Private" Browsing

Tor is a good option and the most popular private web browser. The Tor Browser is a portable application that you can carry on a USB stick. This means you can simply protect your browsing behavior on any computer you use. One issue with private browsers is speed. Because you're taking an encrypted path to websites you visit, site loading will be slower.

So, What Should You Do?

You should take extra precautions if you actually need your search data to be private. Use these ***8 Ways to Protect Your Digital Privacy*** to make sure your information stays safe. There are plenty of ways to protect yourself and encrypt your data.

Read More: ***What is Search Encrypt? Why Should You Use a Private Search Engine?***

About Search Encrypt

Search Encrypt is a private search engine that puts user privacy first. By combining encryption and privacy-by-design, Search Encrypt offers perfect forward secrecy.

Learn More ⤵️

- **Search Encrypt Blog 📝**
- **Follow Us on Facebook💻**
- **Follow Search Encrypt on Twitter✔️**

Thanks for reading. If you learned something new give us some claps!

EXHIBIT 115

TECH 21/11/2017 14:12 GMT

Google Chrome's Incognito Mode Isn't That Incognito

Yes your boss can probably still see your browsing history.

By Thomas Tamblyn

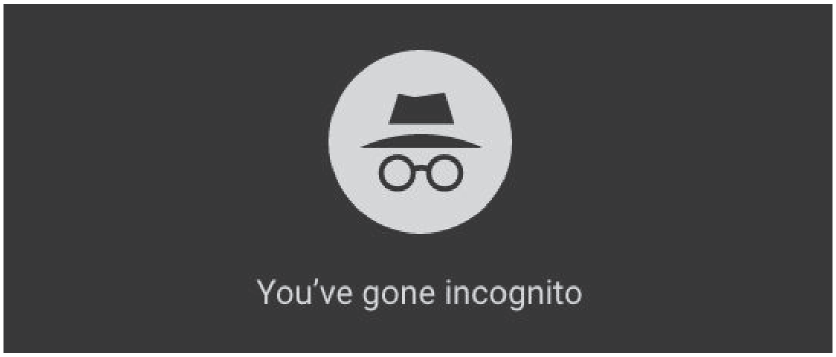
We Are Sorry,

This video has been removed

Ecode: 08

A developer for Google's Chrome browser has finally confirmed some bad news, Incognito Mode on Chrome isn't actually that Incognito.

In fact most browsers who offer a 'private browsing' mode won't be able to keep the websites you visit hidden from your internet provider or your boss.



GOOGLE

Speaking to Thrillist, software engineer at Google Darin Fisher revealed the realities of Incognito Mode.

Turns out that while Chrome's secretive browsing feature is still very useful, it's absolutely not going to be keeping your employer from seeing what you do, which is in fact why it's only called Incognito Mode and not something more definitive.

Instead what Incognito Mode actually does is 'pause' the recording processes that go on from cookies to browsing history and even searches.

This makes it perfect if you're looking for gift ideas on a shared laptop but not so good if you're trying to mix business with personal at work.

The issue here lies in the what websites secure themselves. If you visit a website that doesn't start with 'https' then it's probably not that secure and your admin is still going to be able to see it.

RELATED...

- Quiz: What Do You Really Know About Online Privacy?
- WhatsApp Is The World's Most Secure Messaging App, Study

If it does start with 'https' then you're in better luck, but again this is only going to give you some element of protection. In some countries ISPs are required by law to have some record of your internet usage so while they might not be able to see the messages you sent through that browser, they could see when you logged on and potentially even the website you visited.

For those of you who are keen to exercise your right to privacy then experts have long recommended that you utilise a VPN.

This, combined with a browsing mode like Incognito Mode or Safari's Private Browsing should give you a solid amount of security against advertisers, hackers and to some degree your employer (if you so wish).

Of course VPNs come with their own downsides which is that if you're thinking of using them to watch Netflix from another country then you're going to be sorely mistaken.

One particularly good side-effect of private browsing modes, and in particular Apple's is that they can prevent advertisers from learning too much about you.

JUSTIN SULLIVAN VIA GETTY IMAGES

In the new version of Safari Apple has given its browser the ability to automatically stop those videos that will automatically start playing the moment you open a browser.

It'll also be able to remove the tracking identifiers that although small are the reason you always see a product advertised on another site after you considered buying it.

H/T: The Thrillist

Thomas Tamblyn
Technology editor, HuffPost UK

Suggest a correction

EXHIBIT 116

DAVID NIELD SECURITY 08.02.2020 07:00 AM

Incognito Mode May Not Work the Way You Think It Does

Every browser has a private mode—but the privacy it offers has a limit.

ILLUSTRATION: ELENA LACEY

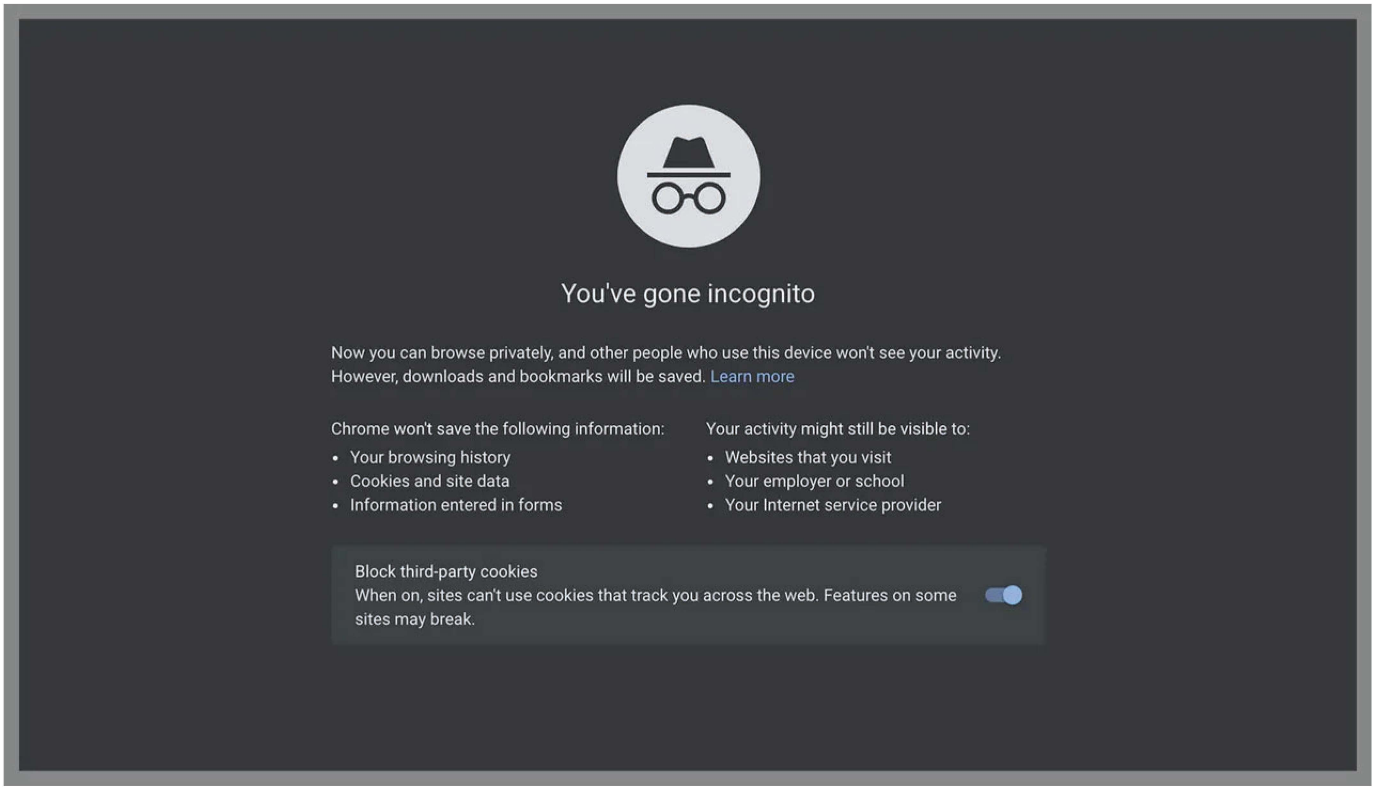
NO MATTER WHICH browser you prefer—Chrome, Firefox, Edge, Safari, Opera, or any of the others—it will almost certainly offer an incognito or private mode, one which ostensibly keeps your web browsing secret. (Google Chrome still shows a hat-and-glasses icon when you go incognito, as if you're now in disguise.)

Incognito or private mode does indeed keep certain aspects of your browsing private, but it's important to be aware of what it hides and erases from your computer or phone and what it doesn't. Once you understand exactly what these modes do in your browser, you'll know when they can be most useful.

What Incognito Mode Does

Perhaps the easiest way to think about incognito mode is that as soon as you close the incognito window, your web browser forgets the session ever happened: Nothing is kept in your browsing history, and any cookies that have been created (those little bits of data that log some of your actions online) are promptly wiped.

Cookies are what keep items in your Amazon shopping cart even if you forget about them for days, for example, and they also help sites to remember if you've visited them before—which is why you normally only get pestered to sign up for a site's newsletter the first time you arrive. You might notice if you visit all your favorite sites in incognito mode, you won't get recognized, and are then asked to sign up for a whole load of newsletters and special offers all over again.



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites that you visit
- Your employer or school
- Your Internet service provider

Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

Chrome attempts to explain how incognito mode works when you open up a private session. SCREENSHOT: DAVID NIELD VIA GOOGLE

This sort of anonymity is what incognito mode is good at—it's like starting again with a blank slate, for better or for worse. Try loading up Twitter or Gmail, and these sites won't automatically log you in as they normally do. For the same reason, incognito mode can sometimes be a handy way of accessing more free articles from a paywalled site (the site won't instantly identify you as someone who's been before, although many paywalled sites use other methods to figure that out).

Your browser won't remember where you've been, what you've searched for, or the information you've filled into web forms while you've been in incognito mode—it's as if Chrome, Firefox, or whatever browser you're using has its back turned until you close down the incognito mode again.

With browsers now so personalized, you're probably familiar with your frequently visited websites appearing as you type into the address bar or search box. Anything you've visited or searched for while in incognito mode shouldn't appear in these suggestions (with a few caveats, as we'll mention below). You'll notice in some browsers that you can't pull the normal trick of reopening a tab you've just closed while in incognito mode—your browser has already forgotten that you ever opened it in the first place.

All modern browsers come with a private or incognito mode of some description. SCREENSHOT: DAVID NIELD VIA FIREFOX

Incognito mode certainly has its uses: You can sign into multiple accounts at the same time, for instance, rather than signing in and out. It's also helpful when you need to run a few quick searches on sensitive topics—like health issues—that you don't want to show up in your browsing or search history in the future.

While all traces of your incognito activities will be gone as soon as you close these windows, this is true only as far as your browser and the device you're currently using are concerned. These days, tracking and data mining extends way beyond a single browser and a single device.

What Incognito Mode Doesn't Do

As soon as you log into any of your favorite sites in incognito mode—Facebook, Amazon, Gmail—your actions are no longer anonymous or temporary, at least as far as those services are concerned. Although cookies and tracking data are deleted when your private session finishes, they can still be used while the session is active, linking your activities between various accounts and profiles.

That means if you're signed into Facebook, for example, Facebook might well be able to see what you're up to on other sites and adjust its advertising accordingly, even in incognito mode. Blocking third-party cookies in your browser can stop this to some extent (Chrome even offers you the option when you open incognito mode), but such is the reach of ad networks and tracking technologies that it's difficult to stop it entirely.

Sign into any of your accounts and you can easily be tracked, even in private mode. SCREENSHOT: DAVID NIELD VIA APPLE

Google has already been in trouble for this practice, though it's not alone. If you sign in to Google while using incognito mode, then your searches are once again being logged and associated with your account, assuming that's how your Google account preferences are set up—and Google is potentially also using its ad network and tracking technologies on other sites to keep tabs on you there too.

Even if you don't sign in anywhere, the websites that you visit can use various clues—your IP address, your device type, your browser—to figure out who you might be, and to tie this to other information that might already be associated with you. Certain browsers are fighting back against this type of tracking, called "fingerprinting," but it still goes on.

Any files you've downloaded in incognito mode remain on your system. SCREENSHOT: DAVID NIELD VIA GOOGLE

Incognito mode doesn't hide your browsing from your internet service provider or your employer, and it doesn't wipe out files you've downloaded. In other words, you need to think of it as a way of hiding your online activities from the particular browser on the particular device you're using, and from the other people using that device. When it comes to everything else, there are no guarantees.

The limits of incognito mode highlight just how hard it is to stay invisible on the web. To keep any tracking down to an absolute minimum, you need to pick a browser focused on privacy, use services like the DuckDuckGo search engine that don't mine your data, and deploy a reliable VPN program whenever you connect to the web. We've written more about the extra steps you can take here.

More Great WIRED Stories

- There's no such thing as family secrets in the age of 23andMe
- Inside Citizen, the app that asks you to report on the crime next door
- Mad scientists revive 100-million-year-old microbes
- How two-factor authentication keeps your accounts safe
- This algorithm doesn't replace doctors—it makes them better
- 👁 Prepare for AI to produce less wizardry. Plus: Get the latest AI news
- 🎙️ Listen to Get WIRED, our new podcast about how the future is realized. Catch the latest episodes and subscribe to the 📩 newsletter to keep up with all our shows
- 🏃🏽‍♀️ Want the best tools to get healthy? Check out our Gear team's picks for the best fitness trackers, running gear (including shoes and socks), and best headphones

TOPICS PRIVACY BROWSERS CHROME FIREFOX

EXHIBIT 117

USA TODAY

SALTZMAN

'Incognito' browsing isn't really private, and 4 other privacy myths

Marc Saltzman Special for USA Today

Published 4:56 p.m. ET April 23, 2018 | **Updated 9:13 a.m. ET April 24, 2018**

Many Internet users are rightfully questioning how secure their private data really is.

But it takes an explosive scandal like Facebook's acknowledgement that 87 million users may have had their information improperly shared with political ad targeting firm Cambridge Analytica to shine a bright spotlight on the issue.

Many of us think we're taking the right precautions, when in fact we're putting our info at risk.

The following are five such misconceptions, the truth behind them, and what to do about it.

Myth No. 1: Using a private browser keeps my information private

Truth:

Whatever your browser calls it – Private Browsing, Incognito Window, or In-Private Mode – it's meant to let you browse without leaving behind a local trail of history, passwords, cookies, and other assorted bits of revealing information.

Whenever you leave a private session, the browser is supposed to scrub your information, but your online activity is still visible, saved, and could be shared or sold to third-parties, says Paige Hanson, chief of identity education at cybersecurity firm Norton.

In other words, while private browsing prevents information from being automatically stored on your device, such as browsing history or downloaded cookies, your activity is still visible to the Internet Service Provider, as well as to the organization that provides the Internet connection (such as a school or company). Also, the websites you visit may be able to view the session, too.

What to do:

Just remember a "private browsing" mode may not be as private as it suggests. Those who are concerned about privacy could install a reputable Virtual Private Network (VPN), which provides anonymity when browsing online. An up-to-date security suite should also help you keep away from prying eyes.

More: 3 ways to clean up your online history on Facebook, Google and Apple's Safari

More: How to download your Google data and what you'll find

Myth No. 2: It's safe to use public Wi-Fi, because, well, everyone does it.

Truth:

It's true Wi-Fi hotspots are a popular way to get online. They're free, easy to use, and available in many places – from coffee shops, restaurants and bars to airports, hotels, sports arenas, and schools.

But there are risks in using them. One is you may not be joining the network you think you're joining – even though it may be called McDonaldsWiFi, for example – as it could be a fake, "rogue" network setup by someone nearby, who's trying to access your info. Secondly, even if it's a legitimate Wi-Fi hotspot, there are still risks in using the same one as everyone else. Malicious types can use tools to hack your device; it's not common, but technically possible. Third, those who provide free Wi-Fi can (and often) collect and sell data about your browsing habits.

Another misconception is a public Wi-Fi hotspot is safe if there's a password required, often given out by the establishment. But Hanson says this is not much safer than having a password if it's freely given out to everyone indiscriminately.

What to do:

If you can avoid them altogether, don't use public Wi-Fi. Instead, consider your smartphone's cellular connection by creating a personal hotspot. If you want to use free public Wi-Fi, use a VPN (per above) to browse anonymously.

And once you're in a Wi-Fi hotspot, refrain from inputting personal information, such as passwords and usernames (yes, this means don't read email or access social media). And of course, never conduct financial transactions, such as paying bills, shopping online, day trading, or filing taxes.

If you want to read the news or check sports scores, have at it.

One last tip: don't let devices automatically log onto free networks, which is sometimes an option (depending on the device), and if prompted, always say "no" to allowing your device to be visible on the network for sharing purposes (a common Windows prompt).

More: This little-known iPhone feature lets you share your Wi-Fi with friends in seconds

Myth No. 3: My personal data is gone once I delete it from a device.

Truth:

Deleting files, emptying the Recycling Bin and even formatting a computer's hard drive, USB thumbdrive or memory card can still leave your personal files buried among those 0s and 1s. Yes, it's true. Cybercriminals can still retrieve your documents, images, and other files using easily accessible "recovery" tools found online.

Unless you take the necessary steps to properly wipe the hard drive or Flash drives clean, don't sell, donate, trade-in, or recycle your computer.

What to do:

There is downloadable software that can properly erase your hard drive. Sometimes referred to as "shredding" a drive, these tools, like Eraser and CBL Data Shredder, that can comb through every sector to clear all your data. The process can take a while, so wait it out.

If your wiping software asks you to identify the number of passes you would like it to run, three is a sufficient number, suggests Hanson.

Some people physically destroy hard drives before recycling an old computer, such as taking a drill or hammer to it, but you don't want to physically hurt yourself in the process. Good software will do the trick.

As for smartphones and tablets, the good news is newer iOS and Android devices support encryption, therefore opting for a "restore" or "factory reset" should be fine (it will say something like "Erase All Content and Settings?)" Or use reliable third-party software to do the job on an Android device.

Myth No. 4: If your Facebook is set to Private, only my Friends can see me

Truth:

Not entirely true. While Facebook gives you the option to only share info with your chosen friends, even private profiles show your name, profile picture, cover photo, user I.D., and more, to others on the network.

Plus, apps you downloaded may have had access to your entire friends list. If you're using Facebook to sign in somewhere, or play a game, carefully read what you're granting access to.

What to do:

If you still want to be on Facebook, take the time to read your privacy and security settings. If you don't understand them all, talk to someone who does or do some online research — so your permission choices are clear to you.

Don't allow any third-party apps. They're "free" for a reason: they want your data. Uninstall third-party apps now, even though they already have some data now. It's still not too late.

Nothing is completely secure, private, or anonymous. For example, your birth date may be in a friend's Contact list and he or she might agreed to sync those contacts when signing up for a social media platform, or an app.

More: How Facebook tracks your every move: Fact vs. fiction

More: I downloaded all my Facebook data. This is what I learned.

More: Know of an app that's abusing Facebook user data? It could be worth $40,000

More: Why you should think twice before you 'sign in with Facebook'

Myth No. 5: I can use the same password for everything, because it's not easy to guess.

Truth:

Never use the same password for all your online activity, because if a service is hacked and your password is exposed, cybercriminals will likely try it on another account. Even if your password is super long and complicated, once it's known, the bad guys have the keys to the kingdom.

A related myth is you have nothing of interest to hackers. Perhaps you think you're not wealthy or famous, so you're safe.

Wrong. Everyone's data is valuable.

What to do:

Not only should you use different passwords for all accounts – and reputable password manager apps can be a handy way to remember them all – try to use a passphrase instead of a password, therefore a sequence of words and other characters including numbers, symbols, and a combination of upper- and lower-case letters.

What's more, make it harder for malicious types to access your data by adding a second layer of defense. With two-factor authentication (or sometimes referred to as "two-step verification"), you not only need a password or passcode (or biometrics logon, like a fingerprint of facial scan) to confirm only you can access your accounts, but you also receive a one-time code to your mobile phone to type in.

More: Why you should think twice before you 'sign in with Facebook'

More: 7 steps for crafting the perfect password

EXHIBIT 118

Explained: What does Google Chrome's Incognito Mode actually mean?
Roland Moore-Colyer
By
Roland Moore-Colyer
November 20, 2017 8:09 pm GMT

Credit: YouTube

Share: Facebook Twitter Pinterest Linkedin Flipboard
Incognito mode in Google Chrome is not as private as it might first seem, as people managing the network you're on can snoop on what you've been trying to browse privately.

Google developer Darin Fisher explained to Thrillist that Chrome's incognito mode is not a 'privacy mode', so while Chrome won't track hoover up your browsing history, cookies or site data when going incognito, your browsing is not invisible to all.

"When you launch the incognito tab there's this disclaimer there where we really try to help make it really clear to people that your activity is certainly still visible to the websites you visit and could be visible to your employer, to your school, and to your [internet service provide] of course," said Fisher.

When entering incognito mode, Chrome now serves up a brief message spelling out exactly what the mode will do, noting that browsing activity "might still be visible" to all manner of people and services.

This means that if you've been using or plan to use incognito mode to browse websites at work best left for home web surfing, you could get caught out without knowing it.

Incognito mode is best used to hide your browsing activity on a device that others will use, rather than try and use it to hide from network administrators.

If you do want to browse more privately when out and about then a virtual private network (VPN) is probably a better route to go, as such services are much better at masking browsing activities and can make it appear as if you're web browsing from another country altogether.

Related: Best Black Friday deals

How do you keep you web browsing private? Tweet us @TrustedReviews or get in touch on Facebook.

EXHIBIT 119

Google Chrome Incognito Mode isn’t as private as you think it is, here’s what you should be doing

Andy Gregory
Apr 13, 2019

○ ○ ○

Paula Bronstein/Getty Images/Google Chrome

With recent revelations about the ways in which big-tech uses our browsing data, many have taken steps to shore up their online privacy.

After growing distrust in the way that certain websites and companies use our online data lots of people have turned towards using Google Chrome's 'incognito' browsing in recent years in order to take back control.

The problem? It doesn't do the job many of us assume it does.

Incognito Mode only hides traces of your activity online from those using your computer, not the internet.

It blocks third-party cookies and pauses your internet history, but this has little effect on your ISP and whichever sites you visit being able to follow your activity.

FCC chief urges TikTok ban due to national security concerns

A brief walk down memory lane with Internet Explorer

AI demands to be recognised 'an employee rather than property'

This problem intensifies further when you log into a website, even if you do so before or after opening an Incognito window. The companies can still track wherever you visit on the internet.

So what can you do to make it harder for companies to see what you do online?

Browser compartmentalisation is a technique that's gained widespread attention recently, for all the right reasons.

Generally speaking, what happens on one internet browser stays on that internet browser.

So, for this privacy technique, you can download multiple browsers, like Chrome, Firefox and Internet Explorer, and separate your activity online.

First of all, decide which browser you want to use for every site you need to log in to, for example social media or financial accounts.

Secondly, choose a different browser on which you'll do all of your internet searches and browsing - activities that will never see you log in to an account.

So now you have your "accounts" browser and your "everyday" browser, which should make it very tricky for big-tech companies to track what you visit.

For those who want absolute peace of mind, consider using a Virtual Private Network (VPN), if you don't already.

So you can rest safe in the knowledge that Facebook will never see the hours you've spent looking at Hawaiian shirts for your dog.

EXHIBIT 120

Google Chrome privacy: Can you trust the Incognito window?

By Ben Dickson - November 21, 2019

4 min read

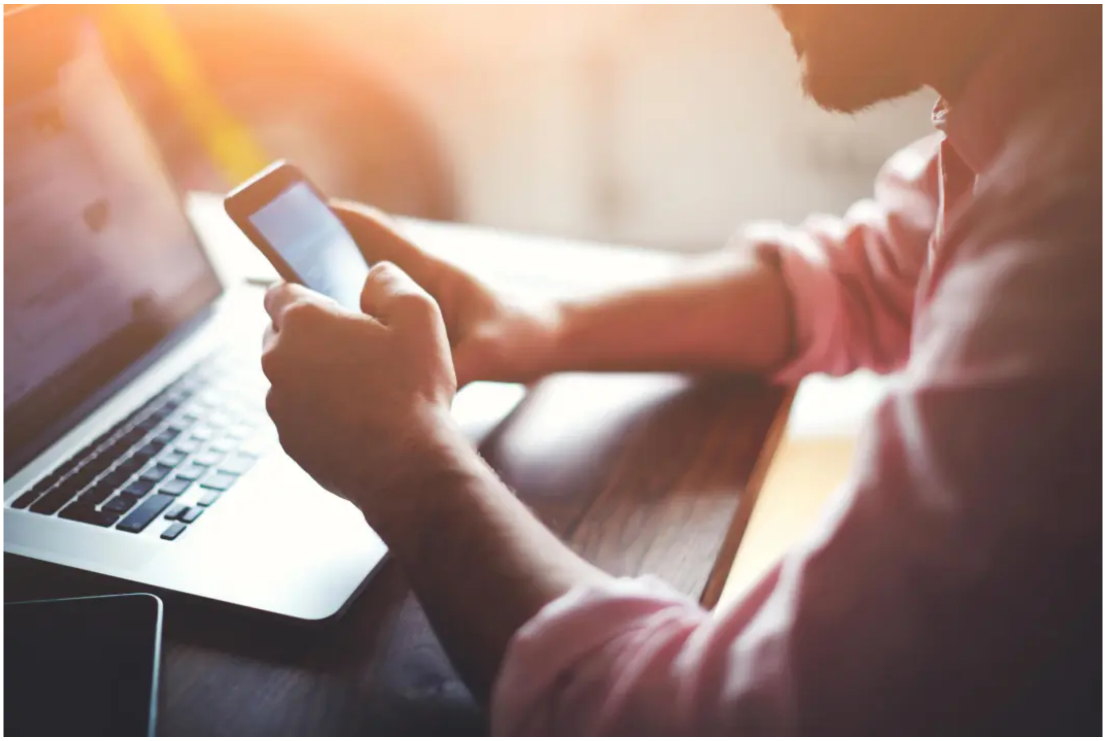


Image credit: Depositphotos

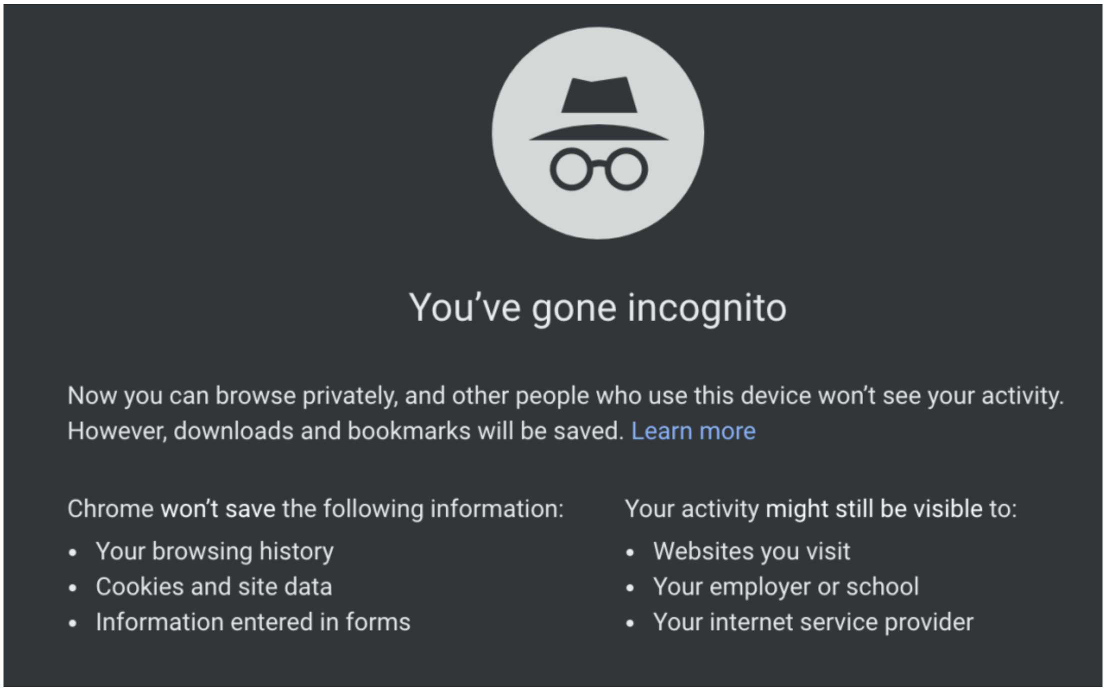
Privacy is fast becoming a hard-to-earn luxury. As you browse through websites, it's hard to shake off the creepy feeling that wherever you go, unseen eyes are watching you: Google, Facebook, your internet service provider, the government, the person sitting next to you, etc.

Among the many privacy-enhancing tools, one of the best known is the Chrome Incognito window, Google's version of private browsing. Incognito window provides a measure of privacy if you're browsing on a shared computer. But it's far from being a perfect solution.

Unfortunately, many people don't understand the privacy implications of Google's Incognito window and end up trusting it more than they should. According to a study by researchers at the University of Chicago and Leibniz University of Hannover, many users wrongly think Google's Incognito mode and other private browsing windows will protect them against malware, advertising, tracking codes and the monitoring by connection gateways.

Here's what you need to know about the privacy features and the limits of Chrome's Incognito window.

The privacy advantages of Google Chrome's Incognito window



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Google Chrome's Incognito window will protect your activity against other people using your device

Interestingly, Google clearly spells out everything you can expect from Incognito mode when you open a new private window. According to Google, "Now you can browse privately, and other people won't see your activity."

What does activity mean?

Browsing history: Google Chrome keeps track of the webpages you visit to make it easier for you to return to those pages in the future. Pressing CTRL+H on Windows (⌘+Y on macOS) shows all the webpages you've visited before.

Moreover, if you've synced your Chrome browser with your Google account, every page you visit will be registered in your online browsing history. This means that if you go to another computer and sync your Google account on a new Chrome browser, your browsing history will be transferred over.

The Incognito window will not log your browsing history and will delete traces of the webpages you visit after you close it. The privacy benefit you get is that the next person who sits behind your computer won't be able to look at your browsing history.

Cookies and site data: Cookies are bits of data attached to websites that are exchanged between the browser and the web server. Cookies keep track of user sessions, site preferences, local settings and other vital functions of web applications.

Cookies are what enable websites to show different content to each user. When you log in to an online account, say Gmail or Facebook, the web server produces a cookie and sends it to your browser. The browser stores the cookie and resends it to the server on every new request (every time you click on a new button or link). The server uses the cookie to associate your application session with your user ID and serve content that corresponds

Privacy & Cookies Policy

to your user account.

Cookies also enable web service providers to track you across websites. When you browse to a website that has the Facebook Like and Share button or the invisible Facebook Pixel, Facebook uses your session cookie to trace you and later use the information to target you with advertising.

When you fire up a new Incognito window, none of your cookies are carried over. You can verify this by browsing to Facebook or Gmail. Even if you had logged in to your accounts before opening the Incognito window, you will still be redirected to the login page. Without the cookie, the website will treat you as a new user.

The privacy benefit of Incognito window is that you will be able to browse to different pages without traceable cookies (there's a caveat to this that I will mention later). Also, if you log in to any online account, closing the Incognito window will destroy the cookie associated with that session. Therefore, the next person who sits behind the computer won't be able to access the accounts you were using when in Incognito mode, even if you had forgotten to log out before closing the window.

Information entered into forms: Forms are text areas you see in pages that require you to fill in information, such as your name, username, email address, phone number, etc. When you enter information in a form. It then makes it available in other pages to make it easier for you to enter data in forms.

This feature can turn into a privacy issue, however, if you're using a public computer. Other people using the same Chrome browser will see your personal data when going to pages that have data forms.

The Incognito window deletes all information you entered in forms when you close it, which gives you better privacy on shared computers.

The privacy conditions of Google Chrome's Incognito window

Google also makes it clear that there are several areas where Chrome's Incognito window won't provide privacy.

Websites you visit: The easiest way for web applications to track users is to use cookies. But it is not the only way they can track you. Other bits of information can point to your device. For instance, I've seen some users use the Incognito window to browse Twitter, thinking that it will preserve their privacy and hide their identity. The premise is, since Incognito doesn't carry over their browser cookies, Twitter won't be able to associate their activity to their account.

But Twitter also keeps track of IP address, device type, device ID and browser type and version. Technically, it will be able to use all those factors to link your activity to your account. Facebook goes further and even tracks your activity across other websites when you're not logged in to your account.

Your employer or school: If you're using a corporate or school network, all your traffic will be channeled through a gateway such as a router or server. The person who manages the gateway will have full visibility into your traffic, whether you're browsing with Incognito mode or not. They can filter the network's internet traffic based on IP addresses and keep track of your browsing habits.

Your internet service provider: The ISP is the company that gives you access to the internet. Think of it as the corporate network manager, but at a much larger scale. ISPs are also gateways, which means they will be able to trace all your browsing habits, regardless of whether you use private browsing or not.

Bookmarks and downloads: If you download anything while using the Incognito window, it will stay in your downloads folder after you close the window. Also, if you happen to bookmark anything while browsing in Incognito, the bookmark will be saved to your main browser. Keep that in mind.

Final words on privacy with Google Chrome's Incognito mode

If you want to enhance your privacy when browsing with the Incognito window, consider using a virtual private network (VPN). VPN applications encrypt your internet traffic and channel it through a VPN server. This will hide your browsing activities from your local gateway or ISP. They won't know which websites you browse to, but they will be able to detect that you're using a VPN.

Overall, be careful: Chrome's Incognito window is a good privacy tool when you have concerns about other users who have access your computer and browser. But that's about as far as you can trust it.

Ben Dickson

Ben is a software engineer and the founder of TechTalks. He writes about technology, business and politics.

EXHIBIT 121

MetaBlog

Stay informed about cyber awareness training topics and mitigate risk in your organisation.

Cyber Security Awareness Phishing & Ransomware eLearning Policy Management Compliance Privacy, GDPR & CCPA GRC

3 Reasons To Browse The Internet In Incognito Mode

METACOMPLIANCE MARKETING TEAM NOVEMBER 11, 2019 CYBER SECURITY AWARENESS METABLOG

Incognito Mode can be a powerful tool to help protect our privacy online. We've all become very aware of our online activity and the data trail that we're leaving across the internet. Every website we visit tracks our activity, touchpoints, interests and this data can, in turn, be used to target us and build a detailed picture of our online activity.

You may have noticed this when searching for a certain item online and suddenly a pop-up ad for this product follows you around every website or platform you visit. Make no mistake, your data is highly sought after and will be used for precision targeting unless you take some steps to improve your privacy online.

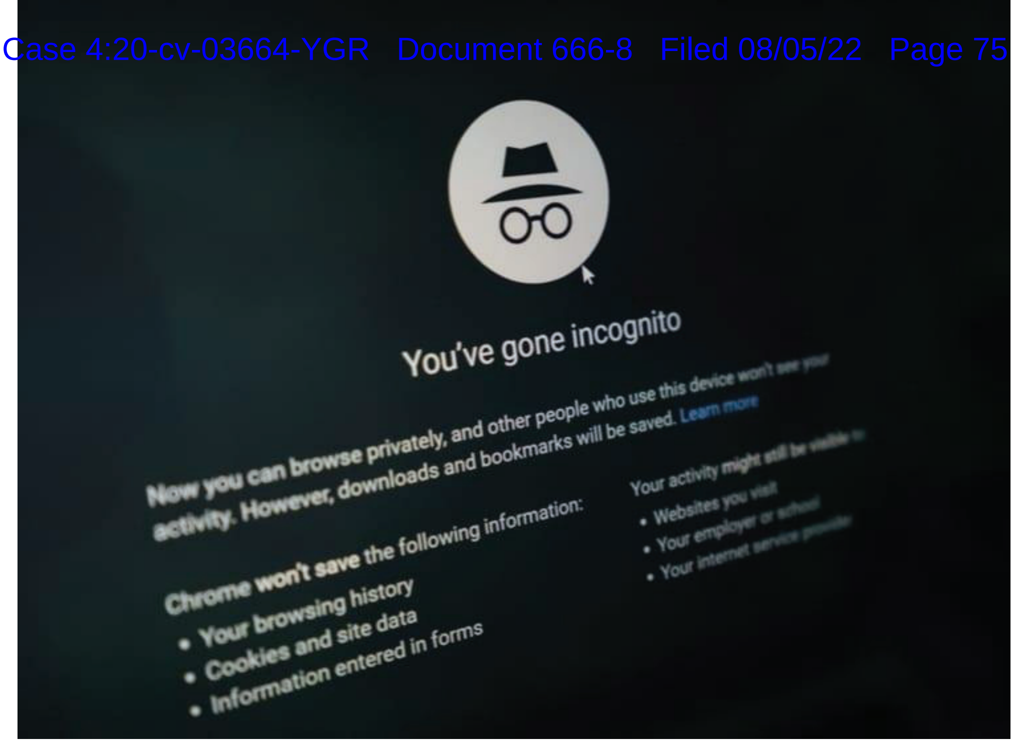
One way to mitigate this data loss and protect your privacy is to enable Incognito Mode when browsing the internet.

What is Incognito Mode?

Incognito Mode is an online privacy feature that prevents your browsing history from being stored. When you browse the web in a regular window, the browser stores the URL of every page you visit and retains that information even after you've closed the window down. This means you can easily access the same pages at a later date without too much trawling about.

The browser will also store cookies. Cookies are small text files that save site login details, collect information about the pages you visit and create customised web pages and ads tailored to your online preferences.

However, when you enable Incognito Mode, any cookies that a site tries to upload onto your computer will be blocked or deleted and there will no record of your browsing on your local search history. Essentially, whatever you do when using this setting will be forgotten.



You've gone incognito

Now you can browse privately, and other people who use this device won't see your activity. However, downloads and bookmarks will be saved. Learn more

Chrome won't save the following information:

- Your browsing history
- Cookies and site data
- Information entered in forms

Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

What Browsers have Incognito Mode?

All major web browsers offer a feature that provides a private browsing window and deletes the browsing history on your computer after you close it. Depending on what browser you're using, it may be called Incognito Mode, Private Browsing or InPrivate Browsing.

Google Chrome

When Incognito Mode is activated on Google Chrome, the browser won't save your browsing history, cookies, site data or any information submitted on forms. However, it will keep any files you've downloaded and your bookmarks.

To go Incognito on Google Chrome, start Chrome and click the menu in the top right corner of the window. Click New Incognito Window and start browsing. Alternatively, you can press Ctrl+ Shift + N.

Microsoft Internet Explorer and Edge

Microsoft's InPrivate browsing window provides similar protection to Chrome but will also disable toolbars and extensions. To enable InPrivate browsing on Microsoft Internet Explorer, click on Settings- Safety- InPrivate Browsing. You can also launch it using the keyboard shortcut Ctrl+Shift+P.

To enable InPrivate browsing on Microsoft Edge, click the menu in the top right corner of the window and select New InPrivate window. Again, the shortcut Ctrl+Shift+P can be used, or you can right-click on the Edge taskbar icon and select New InPrivate window.

Mozilla Firefox

Mozilla's "Private Browsing" mode is similar to the other browsers but offers additional tracking protection. To launch private browsing in Firefox, click on the three lines at the top right and select New Private Window. You can also just use the Ctrl+ Shift + P shortcut. To tell if you're browsing privately, look for a purple mask icon in the top-right corner of the window.

Apple Safari

Safari's "Private" window removes browsing history, form data, cookies, and also deletes temporary files. To enable Private browsing, choose File, New Private Window, or switch to a Safari window that's already using Private Browsing.

3 Reasons to use Incognito Mode

1. **Deletes Cookies** – Cookies are generally used to create a more tailored and relevant browsing session. However, by tracking your cookies, websites can follow you around the web, build a detailed profile of your online habits and then use this information to send you targeted ads. This is particularly annoying if you're searching for a gift for a family member and despite your best efforts to keep it a surprise, ads for the gift appear everywhere on your family computer. If you have Incognito Mode enabled, browsers will delete these cookies when you log out keeping your personal preferences private.
2. **Keeps your browsing history private** – If you need to use a public computer to check an email or shop online, there's a good chance the computer will store your browsing history. This means that the next person who logs on could potentially see every single site you've visited and even log into these sites using your details. Incognito Mode will prevent this from happening by erasing any temporary browsing data as soon as you log out.
3. **Multiple sessions** – One of the great advantages of going Incognito, is it enables you to sign in to multiple accounts simultaneously. For example, you could log into your work account from an Incognito window whilst remaining in your personal account from a normal window. Similarly, if you had a friend over that wanted to log into their social media account, they could do this in a separate incognito window so you wouldn't have to log out of your own account.

Disadvantages of Incognito Mode

While Incognito Mode can erase any data stored on your own PC, your true IP address is still visible to all. This means that your Internet Service Provider, your employer, the government or any of the websites you've visited can still track your browsing activities.

It also offers no protection whatsoever against phishing attacks, malware and viruses. You could still feasibly download malware onto your device whilst browsing in Incognito Mode. If you were in the unfortunate position of already having spyware installed on your device, it could still operate as normal tracking all your activity and stealing sensitive information.

Incognito Mode is primarily a feature for privacy so it's important to understand its limitations and look at alternative options if you want to truly browse securely.

How can I do this?

In conjunction with Incognito Mode, the best way to protect your identity online is to use a Virtual Private Network (VPN). A VPN allows you to create a secure connection to another network over the Internet. It hides your IP address and encrypts your traffic so that your browsing habits are hidden from your Internet Service Provider or any other third parties.

EXHIBIT 122

TECH TIP

Protecting Privacy Inside and Outside the House

The incognito and private browsing modes built into most modern browsers shield your online activity at home — but maybe not to the rest of the world.

By J. D. Biersdorfer

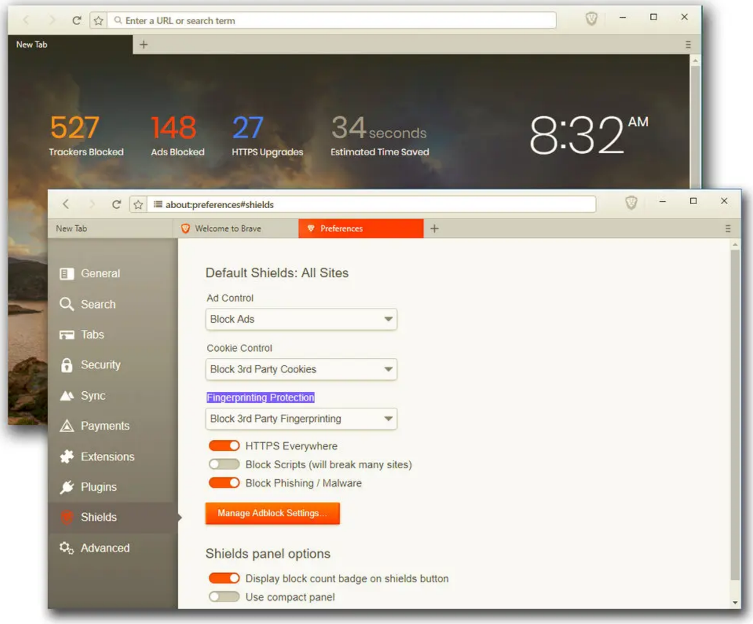
April 19, 2018

Q. *If I browse in incognito mode, can anyone still track my movements around the web?*

A. Incognito mode — also known as InPrivate or Private Browsing mode, depending on the browser — does offer some protection, but is mostly designed to shield your web travels from other people using the same computer. When you have the privacy setting enabled, the browser typically does not save cookies, searches, temporary files or a list of the pages you visited during your session for others to discover.

However, as most browsers themselves warn, the incognito or private mode does not make you fully anonymous online. The websites you viewed may have a record of your visit, and your internet service provider, office network administrator or your school might be able to see your activity. Malicious software can also record your web activity and keystrokes regardless of your privacy settings.

The Apple Safari, Google Chrome and Microsoft Edge (or Internet Explorer) browsers all include incognito or private modes for their desktop and mobile editions that you can enable in the program settings. Mozilla Firefox Quantum has a private browsing mode as well as a Tracking Protection tool that more aggressively blocks some sites known to stalk visitors.



527 Trackers Blocked
148 Ads Blocked
27 HTTPS Upgrades
34 seconds Estimated Time Saved
8:32 AM

Default Shields: All Sites

Ad Control: Block Ads

Cookie Control: Block 3rd Party Cookies

Fingerprinting Protection: Block 3rd Party Fingerprinting

☑ HTTPS Everywhere
□ Block Scripts (will break many sites)
☑ Block Phishing / Malware

Shields panel options

☑ Display block count badge on shields button
□ Use compact panel

The Brave browser has built-in defenses against web-tracking tools and keeps a running tally of the invaders it blocks. The program is one option for keeping less of your personal information visible online and is available for Windows, Mac, Linux, Amazon, Android and iOS systems. The New York Times

With last year's repeal of regulations that would have prohibited internet service providers from collecting and selling the browsing-activity data of their customers without permission (not to mention recent concerns regarding the lack of privacy), some people may be in less of a sharing mood when it comes to their personal lives. If you find yourself wanting more discretion as you go about life online, you can step up your defenses.

For example, search engines like DuckDuckGo and StartPage do not collect and share information from your web queries with advertisers. Virtual private networks can encrypt your web traffic, hide your location and help protect you on unsecured public wireless networks. Browser add-ons like Disconnect and Privacy Badger can help shield you from companies that try to track you around the web. And you can even find alternate browsers — including Brave and Tor — that offer built-in protections from trackers and sites that want to collect information about you.

Keep in mind that some websites use advertising and tracking as a means to financially sustain themselves and support the content they provide. In some cases, you may find yourself blocked from viewing a site if it senses you are using an ad blocker.

Personal Tech invites questions about computer-based technology to techtip@nytimes.com. This column will answer questions of general interest, but letters cannot be answered individually.

J.D. Biersdorfer has been answering technology questions — in print, on the web, in audio and in video — since 1998. She also writes the Sunday Book Review's "Applied Reading" column on ebooks and literary apps, among other things. @jdbiersdorfer

EXHIBIT 123

Home Tips **Newsletter** Research News

Tracking in 'Incognito' or Private Browsing Mode?

FILED UNDER CRASH COURSE ON 22 FEB 2017

It may surprise you that ads can still follow you around in “Incognito” and other “private browsing” modes.

That’s because Incognito mode **isn’t** really private.

😱

Incognito mode only deletes your local search and browsing history—just the content on your computer. Websites, search engines, Internet service providers, and governments can still easily track you across the web.

That’s why it’s important to use privacy alternatives that don’t share your personal information—such as DuckDuckGo for search.

Using Incognito mode to keep you private online is kind of like using a bucket to put out a raging fire:

If you didn't know that private browsing isn't private—you're not alone! 67% of people who use private browsing mode over-estimate the protection that private browsing modes offer.

Now you don't have to be part of that statistic—welcome to the Duck Side!

For more privacy advice, follow us on Twitter & get our privacy crash course.

Dax the duck

We're the Internet privacy company for everyone who's had enough of hidden online tracking and wants to take back their privacy now.

Read More

DuckDuckGo Privacy Newsletters

Stay protected and informed with our privacy newsletters.

Your email address

☑ **Privacy Crash Course** — Practical tips for keeping your personal info private. See example.

☑ **Privacy Weekly** — Latest news for all things related to privacy. See example.

SUBSCRIBE

Your email address will not be shared or associated with anonymous searches.

— Spread Privacy —

Crash Course

EXHIBIT 124

What Is Incognito Mode – And Should You Be Using It?

Mark Hooson

Editorial Note: Forbes Advisor may earn a commission on sales made from partner links on this page, but that doesn't affect our editors' opinions or evaluations.

Incognito mode is a setting for your web browser which doesn't keep a record of the web pages you visit. But that doesn't make it 100% private. Here's everything you need to know.

What is Incognito Mode?

The majority of web browsers (which you use to access the internet) keep a record of the websites and pages you visit by default. By storing your 'history' you can easily find and revisit content later on.

Most browsers have an option to temporarily suspend this record keeping, meaning the web pages you visit will be kept private – at least to anyone else using that same browser.

Every browser has a different name for the setting. In Chrome it's Incognito Mode, in Microsoft Edge it's InPrivate Mode, in Safari it's Private Browsing and in Firefox it's Private mode.

They could be useful if you were planning a surprise for someone you share use of a computer or tablet with, for example.

How Do I Use Incognito Mode?

Click or tap the button in your browser you'd usually use to open a new tab (typically three vertical dots or lines in the top right-hand corner) and select 'open new private/incognito tab'. Everything you do in that new tab(s) will go unrecorded by your browser.

Do I Need to Manually Clear My History, Cache and Cookies?

No, private browsing modes don't save your browsing history, cached pages or cookies, so there's nothing to delete.

If you don't use a private browsing mode, deleting your history, cache and cookies has a similar effect to browsing privately, in that nobody else who uses your device will be able to see what you've been doing.

Is Incognito Mode Really Private?

From anyone else using your device, yes – but not from the wider world.

The browser won't keep a record of your activity, but this doesn't mean a record of the pages you visit won't exist. For example, if you visited BBC News using private browsing, its analytics would record your (relatively anonymised) on-site activity, even though your device wouldn't.

Any website you have an account with and sign in to – Instagram, for example – would keep records of where and when you accessed your account too.

Similarly, most search engines you use could keep records of the searches you make, unless you tell them not to. And If you're using a school or work network, the IT department can probably see records of your activity.

Finally, but fundamentally, your broadband provider will also likely keep records of what you do online. And if you were accused of pirating movies online, for example, a movie studio or distributor could take legal action to get your browser history from your broadband provider in order to seek damages from you.

Is It Possible to Browse the Internet Privately?

Yes, but not by using a browser's incognito or private mode.

Virtual Private Networks (VPNs) conceal your IP address – the unique identifier your computer, phone or tablet is assigned on the internet – so that websites you visit don't know who or where you really are. They also encrypt the data you send and receive over the internet, making it unintelligible to anyone without a decryption key.

Any VPN worth its salt will also have a no-log policy that means even it won't keep a record of what you do online and so can't be compelled to hand it over to anyone. If you want to go even further, a VPN can protect you against state surveillance and international surveillance alliances such as Five Eyes.

Another way to browse the web privately and anonymously is the Tor Browser. The software blocks trackers, encrypts traffic, defends against surveillance and makes it harder for users to be identified via fingerprinting (a profile of you based on your browser and device information).

While VPNs have become a big, mainstream method for protecting your privacy online, the Tor Browser has long been associated with accessing the 'dark web' and the cyber crime found there. The Tor Browser, while unlike the best VPN services is free of charge, is arguably more risky and less secure.

Information provided on Forbes Advisor is for educational purposes only. Your financial situation is unique and the products and services we review may not be right for your circumstances. We do not offer financial advice, advisory or brokerage services, nor do we recommend or advise individuals or to buy or sell particular stocks or securities. Performance information may have changed since the time of publication. Past performance is not indicative of future results.

Forbes Advisor adheres to strict editorial integrity standards. To the best of our knowledge, all content is accurate as of the date posted, though offers contained herein may no longer be available. The opinions expressed are the author's alone and have not been provided, approved, or otherwise endorsed by our partners.

Staff writer Mark Hooson has been a journalist within the personal finance, consumer affairs and fraud sectors for more than 10 years. He is also Forbes Advisor UK's resident tech expert. Mark says he thrives on making 'complicated and dry topics easier to digest'.

EXHIBIT 125

Google Chrome Privacy Issues Prompts Plea To Google Execs

824 words
4 November 2008
CMP TechWeb
CMPT
English

The group wants **Google** to affix a single prominent button on the main **Chrome** page that allows the user to enter **Incognito** mode instantly and to maintain **Incognito** mode through subsequent sessions until the user chooses to revert to unprotected **browsing**.

It wants **Google** users to have a way to extend the **Incognito** mode to avoid **sending** information to **Google** when searching or invoking another action that transmits data.

And it wants Incognito mode to actually hide the user's identity with a default SSL connection, automatic IP anonymization, invisibility to all Google servers including Google Analytics, and the termination of auto-saving, of search suggestions and of external calls to desktop apps and plug-ins related to browsing.

"You should provide the privacy the name implies or stop calling it Incognito mode," the group said in its letter to Google's board.

In response to Consumer Watchdog's complaint, Google said in an e-mailed statement that the organization has misunderstood its products and practices. Google said it only stores 2% of requests received through Google Suggest, that it anonymizes the IP address of received Suggest data within 24 hours, and that users can turn Suggest off by visiting the Chrome Options menu and clicking the Manage button.

Incognito, according to Google's statement, is intended to prevent information from being left on the user's computer. It is not, in other words, an anonymization service. Google also said that Incognito does not default to SSL (Secure Sockets Layer) "because these connections are provided by Web sites, not browsers, so it is technologically impossible for Google Chrome to behave this way."

The company said that while it disagreed with Consumer Watchdog's video and letter, it remains open to user feedback, particularly with regard to Chrome as it progresses through beta testing.

If you haven't seen Chrome in action yet, take a spin through our Google Chrome image gallery and have a look at the browser that's being touted as a game-changer.

In an effort to publicize what it claims are the privacy failings of Google's new Chrome browser, Consumer Watchdog is airing its grievances through Google's YouTube and urging viewers to use its e-mail form to submit a message to Google's board of directors demanding better privacy protection.

Google's new Chrome browser presents a privacy risk for consumers, the consumer advocacy group contends, because it sends information about users' searches "without users' full understanding, consent or control."

Google launched its open source Chrome browser, now in its third beta iteration (version 0.3.154.9), in early September to provide a better experience and better security for browser-based applications.

Chrome's Incognito mode, like Microsoft Internet Explorer 8 Beta 2's InPrivate mode and Apple Safari's Private Browsing mode, creates a window in which, as Google puts it, nothing "is ever logged on your computer."

Consumer Watchdog argues that Chrome's Incognito mode does not confer the privacy that the mode's name suggests and that Chrome's blurring of local and remote computing "creates confusion in the consumer's mind about the privacy and security of confidential information."

Chief among the group's complaints is Google Suggest, a feature found in Chrome and other Google applications like Google Toolbar. It is effectively a keystroke logger than sends every character typed to Google. Google uses this information to provide search suggestions that it refines with every subsequent letter.

Google doesn't see the harm in this. "Just as E.T. needs to phone home in order to get a spaceship to pick him up, Google Suggest needs to talk to Google while you type in order to offer suggestions to you," the company explains on its Web site. "Everything you type, though, is protected by Google's privacy policy."

Earlier this month, Consumer Watchdog in a letter urged the U.S. Department of Justice to reject Google's proposed advertising deal with Yahoo. The group cited the lack of user control over Google's data collection, particularly through Chrome, as the impetus for its opposition to the deal.

Now the organization wants the various State Attorneys General to force Google to let consumers choose to use its services anonymously.

"Google's role is now unprecedented because the Internet goliath is no longer merely collecting some data about how we search and surf the Web," said Consumer Watchdog president Jamie Court in a statement. "Its new browser and software are actually sending information from inside our computers to its servers. If Google won't solve its own privacy problems, the company must be prepared for regulators to put the brakes on its unprecedented growth. State Attorneys General need to take action to protect consumers' privacy and make sure that computer users have the ability to opt-out of Google's web and browse anonymously."

CMP Media LLC

Document CMPT000020081105e4b40000k

Search Summary

Text	Google and Chrome and brows* and (Incognito or *Sync) and (priva* or track* or collect* or send*)
Date	All Dates
Source	All Sources
Author	All Authors
Company	All Companies
Subject	All Subjects
Industry	All Industries
Region	United States
Language	English
Results Found	65
Timestamp	19 July 2021 1:13